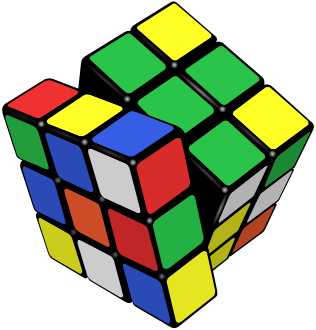
Cryptography in Cyclic Groups (episode 2)



Questions

1. How to find g of order q s.t. q has a prime factor $\geq 2^{256}$?
2. How to determine the order of g?
3. How to test if some element x belongs to $\langle g \rangle$?

Joseph-Louis Lagrange
(1736–1813)

Theorem (Lagrange)

Let G be a finite group and $H \subseteq G$ a subgroup of G.
Then $|H|$ divides $|G|$.

Proof.

- Let $x, y \in G$
- Say that $x \sim y$ iff $\exists h \in H$ (the subgroup) such that $x = yh$
- $\sim$ is an equivalence relation (easy)
- The equivalence class of x is xH
- xH has cardinality $|H|$
  - Multiplication by x is a bijection in G
- Write $[G : H]$ the number of equivalence classes
  - Also known as the "*index* of H in G"
- The equivalence classes form a partition of G
- Therefore $|G| = [G : H] \times |H|$

$\square$

Interesting Consequence

- This is a very general result (all finite groups)

Corollary

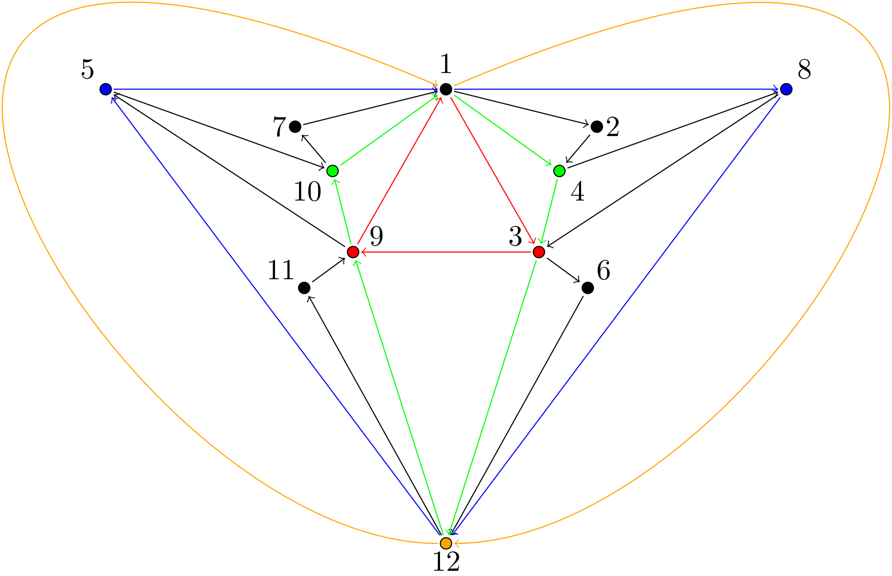
Let $\mathbb{G}$ be a finite group and $g \in \mathbb{G}$.

The order of g divides the order of $\mathbb{G}$.

Proof.

$\langle g \rangle$ is a subgroup of $\mathbb{G}$. Apply Lagrange's theorem. $\square$

Illustration: $\mathbb{F}_{13}^{\times}$



Going Further: Structure of Finite Abelian Groups

Theorem

Let $\mathbb{G}$ be a finite abelian (e.g. commutative) group of finite order n. If k divides n, then $\mathbb{G}$ has a unique subgroup of order k.

- Proof in the special case where $\mathbb{G}$ is cyclic
  - OK for us: $\mathbb{Z}_p^\times$ is cyclic ...
- This is true in general
  - Any finite abelian group is a product of cyclic groups
  - (too complicated)

Proof (existence).

- Write $\mathbb{G} = \langle g \rangle \rightsquigarrow g$ has order n
- We claim that $h := g^{\frac{n}{k}}$ has order k
  - $h^k = g^n = 1$
  - If $0 \leq i < k$, then $h^i = g^{i\frac{n}{k}} \neq 1$ because g has order n

$\square$

Proof (unicity).

- Suppose that $h \in \mathbb{G}$ has order $k > 0$
- We claim that $\langle h \rangle = \langle g^{\frac{n}{k}} \rangle$
- $\mathbb{G}$ is cyclic $\implies h = g^x$ (for some x)
- $h^k = 1 \iff g^{kx} = 1 \iff kx \equiv 0 \mod n$ (g has order n)
- Because k divides n, we find that x is a multiple of $\frac{n}{k}$
- Therefore $h \in \langle g^{\frac{n}{k}} \rangle$ and $\langle h \rangle \subseteq \langle g^{\frac{n}{k}} \rangle$
- Both groups have the same order: $\langle h \rangle = \langle g^{\frac{n}{k}} \rangle$

$\square$

Generators in $\mathbb{Z}_p^\times$

Let q denote the order of g modulo p

- $\mathbb{Z}_p^\times$ has order $p - 1$
  - Notice that $p - 1$ is even
  - $\{-1, 1\}$ is indeed a subgroup of order 2
- Therefore (Lagrange's theorem) q divides $p - 1$
  - $\rightsquigarrow$ *Considerably restricts* the possible values of q
- q has a large prime factor $\Rightarrow p - 1$ has a large prime factor
- $\mathbb{Z}_p^\times$ contains elements of order $p - 1$
  - *Non-trivial theorem* (no proof given here)
  - This means that $\mathbb{Z}_p^\times$ is cyclic
  - An element of order $p - 1$ is called a **primitive root** mod p

Checking the Order of a Generator

Problem

- Someone "promises" you that g has order q modulo p
- Can you verify that it is true?

Validation?

- Check that q divides $p - 1$
- Check that $g \neq 1$
- Check that $g^q = 1$ (necessary, **not sufficient**)
  - This proves that the actual order of g divides q
  - It could be smaller than q
- Special case: the previous test is sufficient if q **is prime**

Checking the Order of a Generator

Problem

- Someone "promises" you that g has order q modulo p
- q is **not prime** (relevant case: primitive roots)

Validation?

- Let ℓ denote the actual order of g
- Check that $g^q = 1$ (necessary, **not sufficient**)
  - This proves that ℓ divides q
  - Write $q = \ell r$
- Suppose $\ell < q$ ($r \neq 1$)
  - Let f be a prime factor of r (and thus of q)
  - Then $g^{\frac{q}{f}} = g^{\frac{q}{r}\frac{r}{f}} = g^{\ell\frac{r}{f}} = 1^{\frac{r}{f}} = 1$
- Contrapositive:
  - $g^{\frac{q}{f}} \neq 1$ for each prime factor f of $q \Longrightarrow g$ has order q

This procedure requires knowledge of the factorization of q

Application: the "Oakley Groups" (RFC 2412 and 3526)
Standardized Groups for the Masses

$$p = 2^{2048} - 2^{1984} - 1 + 2^{64} \times \left([2^{1918}\pi] + 124476 \right)$$
$$g = 2$$

Claim : g has order $p-1$ modulo p

Proof.

- Let q denote the order of g
- $\ell = (p-1)/2$ is also prime
  - p is a *Sophie Germain* prime or a *safe* prime
- Therefore $q \in \{2, \ell, 2\ell\}$
- $g^2 \neq 1$ and $g^\ell \neq 1$, therefore g has order $p-1$

$\square$

Conclusion: $\mathbb{Z}_p^\times = \langle 2 \rangle$

Creating Generators of Prime Order in $\mathbb{Z}_p^\times$ — Schnorr's Trick

Procedure

1. Choose a 256-bit prime q
2. Pick a random 1792-bit integer k
3. Set $p = 1 + kq$
4. If p is not prime, go back to 2.
5. Pick a random x modulo p
6. Set $g \leftarrow x^k$
7. If $g = 1$, go back to 5.
8. g has (prime) order q modulo p

Proof.

- $g^q = x^{p-1} = 1$
  - By Fermat's little theorem
- Therefore, if $g \neq 1$, then g has order q
  - cf. previous slides (easy case: q is prime) □

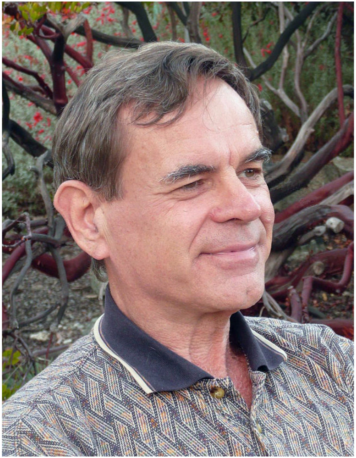
Digression: Primality Certificates
1975

If g has order $n-1$ modulo n, then n is prime

- $\langle g \rangle \subseteq \mathbb{Z}_n^\times$
- g has order $n-1$, *therefore* $|\mathbb{Z}_n^\times| = n-1$
- All integers except zero are invertible modulo n
- n does not have any non-trivial divisor
- n is prime

- providing g of order $n-1$ proves that n is prime
- Checking the order of g requires the factorization of $n-1$
- Certificate of n =
  1. g
  2. Factorization of $n-1$
  3. Certificates of the prime factors (recursively)
- Conclusion: PRIMES $\in$ NP

Digression: Primality Certificates
1975



Vaughan Pratt
(1944–)

DDH Can be Easier than CDH

Let g be a **primitive root** modulo p

- **DLOG** and **CDH** are (presumably) hard in $\mathbb{Z}_p^\times$
- But **DDH** is easy in $\mathbb{Z}_p^\times$!!!
- Argument given around 1800

Leonhard Euler
1707–1783

Adrien-Marie Legendre
1752–1833

Quadratic Residuosity

Definition (Quadratic Residue)

$x \in \mathbb{Z}_p^\times$ is a **quadratic residue** $\Leftrightarrow$ x is a square $(\exists y.\ x = y^2)$

- $QR(\mathbb{Z}_p^\times) = \{x \in \mathbb{Z}_p^\times \mid \exists y \in \mathbb{Z}_p^\times . x = y^2\}$
- $\overline{QR}(\mathbb{Z}_p^\times) = \{x \in \mathbb{Z}_p^\times \mid \forall y \in \mathbb{Z}_p^\times . x \neq y^2\}$

- "Fun" : $25^2 = 5 \mod 31$

Important because...

It is easy to test if $x \in \mathbb{Z}_p$ is a quadratic residue

How Many Quadratic Residues?

Observation

- Suppose $x^2 \equiv y^2 \bmod p$
  $\implies (x-y)(x+y) \equiv 0 \bmod p$
  $\implies x \equiv \pm y \bmod p$
- $(p-1)/2$ distinct pairs $\{x, -x\}$ with $x \neq 0$
  $\rightsquigarrow$ $(p-1)/2$ distinct quadratic residues

More structure

- $QR(\mathbb{Z}_p^\times)$ is the **subgroup** of $\mathbb{Z}_p^\times$ of order $(p-1)/2$
  - 1 is a QR
  - The product of QRs is a QR $\quad a^2b^2 = (ab)^2$
  - The inverse of a QR is a QR $\quad \left(a^2\right)^{-1} = \left(a^{-1}\right)^2$
- $\overline{QR}(\mathbb{Z}_p^\times)$ is not a **subgroup** of $\mathbb{Z}_p^\times$
  - Because 1 is a QR

Quadratic Residuosity (cont'd)

Lemma

Multiplication by a non-QR is a bijection between $QR(\mathbb{Z}_p^\times)$ and $\overline{QR}(\mathbb{Z}_p^\times)$.

Proof.

Let $x \in QR(\mathbb{Z}_p^\times)$ and $\alpha \in \overline{QR}(\mathbb{Z}_p^\times)$. Write $x = y^2$.

- Write $\mathcal{M}_\alpha : x \mapsto \alpha x$
- $\mathcal{M}_\alpha^{-1} = \mathcal{M}_{\alpha^{-1}}$ ($\mathbb{Z}_p^\times$ is a group)
- Suppose $x\alpha = z^2$. Then $\alpha = z^2 x^{-1} = \left(zy^{-1}\right)^2 \rightsquigarrow \alpha$ is a QR!
  $\rightsquigarrow$ $\mathcal{M}_\alpha$ sends $QR(\mathbb{Z}_p^\times)$ to $\overline{QR}(\mathbb{Z}_p^\times)$
- $\left|QR(\mathbb{Z}_p^\times)\right| = \left|\overline{QR}(\mathbb{Z}_p^\times)\right|$ and $\mathcal{M}_\alpha$ is injective
  $\Longrightarrow$ $\mathcal{M}_\alpha$ is a bijection between the two sets

$\square$

$\Longrightarrow$ $QR \times \overline{QR} = \overline{QR}$

$\Longrightarrow$ $\overline{QR} \times \overline{QR} = QR$

Proposition

Let g be a primitive root modulo $p > 2$. Then

$$g^x \text{ is a quadratic residue} \iff x \equiv 0 \bmod 2$$

Proof.

$\Leftarrow$ Trivial. $x \equiv 0 \bmod 2 \Rightarrow \exists y.x = 2y \Rightarrow g^x = g^{2y} = (g^y)^2$

$\Rightarrow$ Suppose that $g^x = \alpha^2$

- g is a primitive root: $\exists y.\alpha = g^y$

$\rightsquigarrow$ $g^x = \alpha^2 = (g^y)^2 = g^{2y}$

- Therefore (lemma from last week)

$$x \equiv 2y \bmod p-1 \quad \Rightarrow \quad \exists k.x = 2y + k(p-1)$$

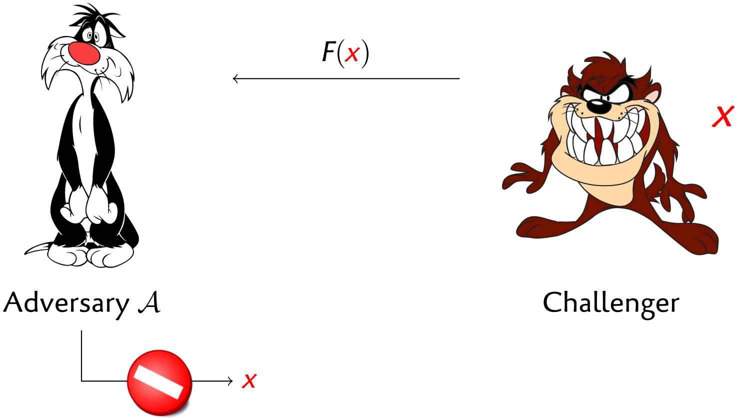
- p is odd $\rightsquigarrow p - 1 = 2\ell$, so $x = 2(y + k\ell)$
- x is even

$\square$

One-Way Functions?

Exponentiation mod p : $x \mapsto g^x$

- I claimed that it is one-way...
  - $\mathcal{A}$ does not recover x from $F(x)$



One-Way Functions?

Exponentiation mod p : $x \mapsto g^x$

- I claimed that it is one-way...
  - $\mathcal{A}$ does not recover x from $F(x)$
- Could $\mathcal{A}$ recover **one bit** $P(x)$ of information about x?

$F(x)$

x

Adversary $\mathcal{A}$

Challenger

$P(x)$

Legendre Symbol and Euler's Criterion

Definition (Legendre Symbol)

Let p be an odd prime number.

$$\left(\frac{a}{p}\right) \overset{def}{=} \begin{cases} 1 & \text{if } a \text{ is a quadratic residue mod } p \\ 0 & \text{if } a = 0 \\ -1 & \text{if } a \text{ is a not quadratic residue mod } p \end{cases}$$

- (just a weird notation for this specific function)
- We have shown earlier that $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

Theorem: Euler's Criterion

$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \mod p$

Weak Bits of the Discrete Logarithm

Exponentiation mod p : $x \mapsto g^x$

With g a primitive root modulo p

$\xleftarrow{g^x}$

x

Adversary $\mathcal{A}$

Challenger

$\longrightarrow$ $x \mod 2$

(Euler's criterion)

Euler's Criterion: $p > 2$ prime $\Rightarrow \left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \mod p$

Proof.

Let's work inside the finite field $\mathbb{Z}_p$.

$$P(X) = X^{p-1} - 1 = \left(X^{\frac{p-1}{2}}\right)^2 - 1 = \underbrace{\left(X^{\frac{p-1}{2}} - 1\right)}_{P_1(X)} \underbrace{\left(X^{\frac{p-1}{2}} + 1\right)}_{P_{-1}(X)}$$

1. α is a QR $\Longrightarrow \alpha^{\frac{p-1}{2}} \equiv 1 \mod p$
   Let $\alpha = \beta^2$ be a quadratic residue. Then
   $$P_1(\alpha) = P_1\left(\beta^2\right) = \left(\beta^2\right)^{\frac{p-1}{2}} - 1 = \beta^{p-1} - 1 = 0$$
   (last step by Fermat's little theorem — everything mod p)
2. α is not a QR $\Longrightarrow P_1(\alpha) \neq 0$
   Note that $P_1(0) = -1$, so that $P_1(X) \neq 0$
   $P_1(X)$ vanishes over the $(p-1)/2$ quadratic residues
   $\deg P_1 = (p-1)/2 \rightsquigarrow P_1$ cannot have any more roots

Euler's Criterion: $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \mod p$

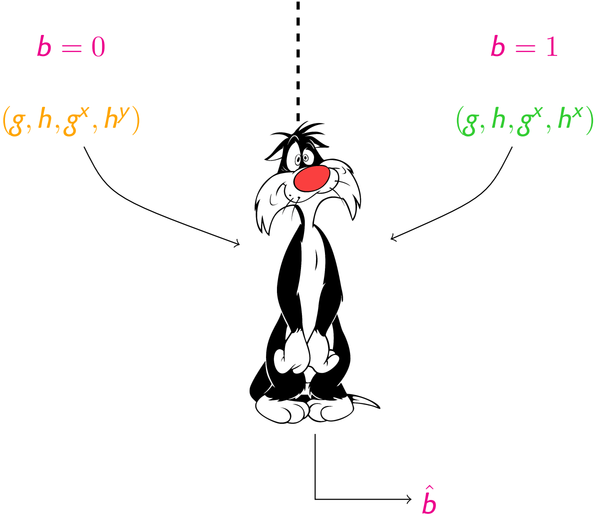
Proof.

$$P(X) = X^{p-1} - 1 = \left(X^{\frac{p-1}{2}}\right)^2 - 1 = \underbrace{\left(X^{\frac{p-1}{2}} - 1\right)}_{P_1(X)} \underbrace{\left(X^{\frac{p-1}{2}} + 1\right)}_{P_{-1}(X)}$$

1. α is a QR $\Longrightarrow \alpha^{\frac{p-1}{2}} = 1$
2. α is not a QR $\Longrightarrow P_1(\alpha) \neq 0$
3. α is not a QR $\Longrightarrow \alpha^{\frac{p-1}{2}} = -1$
    - Fermat's little theorem $\Rightarrow P(\alpha) = 0$
    - $P_1(\alpha) \neq 0 \Longrightarrow P_{-1}(\alpha) = 0$
    - (everything mod p again)

$\square$

Reminder: Decisional Diffie-Hellman (DDH)



- Distinguisher must tell if he is in "world $b = 0$"...
- ... or in "world $b = 1$"

Reminder: Decisional Diffie-Hellman (DDH)

$b = 0$

(g, h, g^x, h^y)

$b = 1$

(g, h, g^x, h^x)

g^x reveals $x \bmod 2$

$$\left(\frac{h^x}{p}\right) = \left(\frac{h}{p}\right)^x = \left(\frac{h}{p}\right)^{x \bmod 2}$$

Inconsistency $\Longrightarrow b = 0$

$\hat{b}$

- Distinguisher must tell if he is in "world $b = 0$"...
- ... or in "world $b = 1$"

Reminder: Decisional Diffie-Hellman (DDH)

$b = 0$

$b = 1$

(g, h, g^x, h^y)

(g, h, g^x, h^x)

g^x reveals $x \bmod 2$

$$\left(\frac{h^x}{p}\right) = \left(\frac{h}{p}\right)^x = \left(\frac{h}{p}\right)^{x \bmod 2}$$

Inconsistency $\Longrightarrow b = 0$

$\Pr(\text{Inconsistency} \mid b = 0) = 0.5$

(consider the 8 possible cases)

$\hat{b}$

- Distinguisher must tell if he is in "world $b = 0$"...
- ... or in "world $b = 1$"

Reminder: Decisional Diffie-Hellman (DDH)

$b = 0$

(g, h, g^x, h^y)

$b = 1$

(g, h, g^x, h^x)

g^x reveals $x \bmod 2$

$$\left(\frac{h^x}{p}\right) = \left(\frac{h}{p}\right)^x = \left(\frac{h}{p}\right)^{x \bmod 2}$$

Inconsistency $\Longrightarrow b = 0$

$\Pr(\text{Inconsistency} \mid b = 0) = 0.5$

(consider the 8 possible cases)

1 if no inconsistency detected

- Advantage 0.5

Computing Square Roots

Suppose x is a QR $\rightsquigarrow x = y^2$

If $p \equiv 3 \bmod 4$

- $(p+1)/4$ is an integer, and we find:

$$\left(x^{\frac{p+1}{4}}\right)^2 = x^{\frac{p+1}{2}} = y^{p+1} = y^2 y^{p-1} = y^2 = x$$

- $(p-1)/2$ is odd $\rightsquigarrow$ -1 is a non-RQ
  $\Longrightarrow$ Deterministic algorithm that finds a non-RQ

If $p \equiv 1 \bmod 4$

- Computing square roots is polynomial (but complicated)
  - Nice challenge for the TME
- Requires finding a non-RQ. How to do this?

Application: the Rabin Trapdoor One-Way Function (1978)

Private key

- p, q: two (large) prime numbers with $p, q \equiv 3 \bmod 4$

Public key

- $N = pq$ ("Blum integer")

Operation

Evaluation $F(x) := x^2 \bmod N$

Inversion

1. Compute square roots $\pm u \bmod p$ (easy case)
2. Compute square roots $\pm v \bmod q$ (easy case)
3. Get square roots mod N using the CRT

$\rightsquigarrow$ 4 possible preimages

The Rabin Trapdoor One-Way Function: Security

Theorem

Factoring *is hard* $\iff$ *the Rabin function is* ***one-way***

Proof.

$\Longleftarrow$ Trivial (factoring is easy $\Longrightarrow$ broken)

$\Longrightarrow$
- Suppose the Rabin function is not one-way
  - There is an efficient (randomized) $\mathcal{A}$ that inverts it
  - $\mathbb{P}\left[x \leftarrow \mathcal{A}(N, y), x^2 \equiv y \bmod N\right]$ is non-negligible

- Factoring algorithm:
  1. Pick random $x \bmod N$
  2. $z \leftarrow \mathcal{A}(N, x^2)$
  3. If $z^2 \not\equiv x^2 \bmod N$, abort ($\mathcal{A}$ failed)
  4. If $z \equiv \pm x \bmod N$, abort (proba 0.5)
  5. Return $\mathrm{GCD}(N, z - x)$

N does not divide $z - x$ or $z + x$, but N divides $(z - x)(z + x)$

$\square$