

MPRI – Cours 2.12.2



F. Morain



Groups and applications

2016/09/12-19

The slides are available on <http://www.lix.polytechnique.fr/Labo/Francois.Morain/MPRI/2016>

Contents

- I. Introduction
- II. Algorithms for generic groups
- III. The ring $(\mathbb{Z}/N\mathbb{Z})^*$
 - A) General results
 - B) Application to primality proving
 - C) Application to factorization: Pollard's $p - 1$
- IV. Finite fields
 - A) General results
 - B) Application to primality proving
- V. Discrete logarithms for generic groups

I. Introduction

Why groups? finite groups are used everywhere in crypto (and elsewhere).

Which tasks?

- representing elements;
- drawing elements at random;
- efficient group laws;
- computation of cardinality;
- structure (with generators);
- etc.

Some groups

- $(\mathbb{Z}/N\mathbb{Z})^*$;
- finite fields \mathbb{F}_{q^n} and subfields;
- algebraic curves (elliptic, hyperelliptic, any genus) over finite fields;
- class groups;
- etc.

II. Algorithms for generic groups

$(G, \circ, 1_G)$, Abelian, finite, of order N ; computable \circ .

Def. $\text{ord}_G(a) = \min\{k > 0, a^k = 1_G\}$.

Thm. (Lagrange) $\text{ord}_G(a) \mid N$.

Coro. $a^{-1} = a^{N-1}$.

Def. $\text{Exp}(G) = \min\{k > 0, \forall a \in G, a^k = 1_G\}$.

Prop.

1. $\text{Exp}(G) \mid N$;
2. $\text{Exp}(G) = \text{lcm}(\text{ord}_G(a), a \in G)$.

It can happen that $\text{Exp}(G) < N$, see later.

Finding the order of an element

Pb. $G = \langle g \rangle$, $N = \text{ord}(g)$; what is the order ω of a in G ?

Thm. (Lagrange) $\omega \mid N$.

Rem. If N is small, we can enumerate in $O(N)$ or its divisors.

Prop. a is of order ω if and only if

- i) $a^\omega = 1_G$;
- ii) for all prime $p \mid \omega$, $a^{\omega/p} \neq 1_G$.

Proof:

In practice, if N and its factorization are known, easy.

What if we don't know N (completely)? E.g., (hyper)elliptic curves.

Baby-steps giant-steps

Fundamental algorithm in ANT/crypto; due to Shanks.

Write:

$$\omega = cu + d, \quad 0 \leq d < u, \quad 0 \leq c < N/u.$$
$$a^\omega = 1 \Leftrightarrow (a^{-u})^c = a^d.$$

Number of group operations: $C_o = u + N/u$ minimized for $u = \sqrt{N}$, hence $2\sqrt{N}$ group operations.

Set operations: u insertions in \mathcal{B} and N/u membership tests in the worst case.

$\Rightarrow \mathcal{B}$ must be a hash table, where both operations take $O(1)$.

Complexity: $O(\sqrt{N})$ in time and space.

Function $BSGS(G, g, N, a)$

Input : $G \supset \langle g \rangle$, g of order N

Output: $\omega = \text{ord}(a)$

$u \leftarrow \lceil \sqrt{N} \rceil$;

// Step 1 (baby steps)

initialize a table \mathcal{B} for storing u pairs (elt of G , int $< N$);

store(\mathcal{B} , $(1_G, 0)$);

$H \leftarrow a$; store(\mathcal{B} , $(H, 1)$);

for $d := 2$ **to** $u - 1$ **do**

$H \leftarrow H \circ a$; store(\mathcal{B} , (H, d));

// Step 2 (giant steps)

$H \leftarrow H \circ a$; $f \leftarrow 1/H = a^{-u}$;

$H \leftarrow 1_G$;

for $c := 0$ **to** N/u **do**

 // $H = f^c$

if $\exists (H', d) \in \mathcal{B}$ such that $H = H'$ **then**

 // $H = f^c = a^d$ hence $\omega = cu + d$

return $cu + d$;

$H \leftarrow H \circ f$;

Exo1-1. Decrease the average time by remarking that $c \approx N/(2u)$ on average.

Exo1-2. What if computing $1/x$ is free?

Exo1-3. Design a variant which takes $O(\max(c, d))$ operations. What is its average running time?

III. The ring $(\mathbb{Z}/N\mathbb{Z})^*$

A) General results

Thm. \mathbb{Z} is an euclidean domain: $a = bq + r, 0 \leq r < |b|$.

Def. $\mathbb{Z}/N\mathbb{Z} = \{0, 1, \dots, N - 1\}$ set of equivalence classes of $x \mathcal{R}_y \iff x - y \in N\mathbb{Z}$ or $x \equiv y \pmod{N}$; add ring operations.

Prop. $(\mathbb{Z}/N\mathbb{Z})^* = \{x \in \mathbb{Z}/N\mathbb{Z}, \exists y, xy \equiv 1 \pmod{N}\}$
 $= \{x \in \mathbb{Z}/N\mathbb{Z}, \gcd(x, N) = 1\}$.

Thm. (Euler totient function)
 $\varphi(N) := \text{Card}((\mathbb{Z}/N\mathbb{Z})^*) = \prod_{i=1}^k \varphi(p_i^{\alpha_i}) = \prod_{i=1}^k p_i^{\alpha_i-1} (p_i - 1)$ where
 $N = \prod_{i=1}^k p_i^{\alpha_i}$.

Thm. (Carmichael function) $\text{Exp}((\mathbb{Z}/N\mathbb{Z})^*) = \lambda(N) = \text{lcm}_{i=1}^k \lambda(p_i^{\alpha_i})$
 where

$$\lambda(p_i^{\alpha_i}) = \begin{cases} \varphi(p_i^{\alpha_i}) = p_i^{\alpha_i-1} (p_i - 1) & \text{if } p_i \text{ odd or } \alpha_i \leq 2, \\ 2^{e-2} & \text{if } e \geq 3. \end{cases}$$

More properties

Thm. $\mathbb{Z}/N\mathbb{Z}$ is a field iff N is prime.

Thm. $\mathbb{Z}/N\mathbb{Z} \simeq \prod_{i=1}^k \mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}$.

Rem. Chinese Remaindering Theorem (CRT) Given $(x_i)_{1 \leq i \leq k}$ with $x_i \in \mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}, \exists$ unique $x \in \mathbb{Z}/N\mathbb{Z}, x \equiv x_i \pmod{p_i^{\alpha_i}}$ for all i .

Thm. $(\mathbb{Z}/N\mathbb{Z})^*$ is cyclic iff $N = p^\alpha$ or $2p^\alpha$ for odd p , or $N = 2, 4$.

Justification of RSA

Prop. If N is squarefree, then for all $a \in \mathbb{Z}, a^{\lambda(N)+1} \equiv a \pmod{N}$.

Proof:

Coro. RSA is valid: for all $x, x^{ed} \equiv x \pmod{N}$.

Proof:

B) Application to primality proving

Thm.(Fermat) N is prime if and only if $(\mathbb{Z}/N\mathbb{Z})^*$ is cyclic of order $N - 1$:

$$\left. \begin{array}{l} a^{N-1} \equiv 1 \pmod{N} \\ \forall p \mid N-1, a^{\frac{N-1}{p}} \not\equiv 1 \pmod{N} \end{array} \right\} \Rightarrow N \text{ is prime}$$

Certificate: $(N, \{p \mid N-1\}, a) \Rightarrow \text{isPrime?} \in \text{NP}$.

Thm. (Pocklington, 1914) Let s s.t. $s \mid N-1$

$$\left. \begin{array}{l} a^{N-1} \equiv 1 \pmod{N} \\ \forall q \text{ prime} \mid s, \gcd(a^{\frac{N-1}{q}} - 1, N) = 1 \end{array} \right\} \Rightarrow \forall p \mid N, p \equiv 1 \pmod{s}$$

Coro. $s > \sqrt{N} \Rightarrow N$ is prime.

Example of use

Hyp. We know how to find all prime factors < 20 .

$$\begin{aligned} N_0 &= 100003, & N_0 - 1 &= 2 \times 3 \times 7 \times N_1, \\ N_1 &= 2381, & N_1 - 1 &= 2^2 \times 5 \times 7 \times 17 \end{aligned}$$

p	2	5	7	17
$3^{(N_1-1)/p} \pmod{N_1}$	2380	1347	1944	949

$\Rightarrow N_1$ is prime

$$s = N_1 > \sqrt{N_0}$$

$$2^{N_0-1} \equiv 1 \pmod{N_0}, \gcd(2^{(N_0-1)/N_1} - 1, N_0) = 1$$

$\Rightarrow N_0$ is prime

Rem. We have got a (recursive) primality proof of depth $O(\log N)$.

Compositeness

Fermat: if $\gcd(a, N) = 1$, then $a^{N-1} \equiv 1 \pmod{N}$.

But: $2^{340} \equiv 1 \pmod{341}$: pseudoprime to base 2 (psp-2).

Thm. There exists an infinite number of psp-2 numbers.

Def. $P(N) = \#\{a \in (\mathbb{Z}/N\mathbb{Z})^*, a^{N-1} \equiv 1 \pmod{N}\}$.

Thm. If $N = \prod_i p_i^{\alpha_i}$, $P(N) = \prod_i \gcd(p_i - 1, N - 1)$.

Proof: ■

Thm. There exists an infinite number of psp- a numbers for all possible a 's (Carmichael numbers: 561, etc.), i.e., $P(N) = \varphi(N)$.

The test

function isComposite(N)

1. Choose a at random in $\mathbb{Z}/N\mathbb{Z} - \{0\}$.
2. Compute $g = \gcd(a, N)$; if $g > 1$, then return (yes, $g \mid N$).
3. if $a^{N-1} \not\equiv 1 \pmod{N}$, then return (yes, a)
otherwise return I don't know.

Cost. $O((\log N)M(\log N))$; typically $O((\log N)^3)$, asymptotically $\tilde{O}((\log N)^2)$.

Prop. Proba("I don't know") = $P(N)/(N-1)$.

Proof. Probability of yes is:

$$\left(1 - \frac{\varphi(N)}{N-1}\right) + \frac{\varphi(N)}{N-1} \left(1 - \frac{P(N)}{\varphi(N)}\right). \square$$

Rem. if N is prime, proba is 1...!

Improvement: Solovay-Strassen

Euler: if N is prime and $\gcd(a, N) = 1$, then $a^{(N-1)/2} \equiv \left(\frac{a}{N}\right) \pmod{N}$.

Pb: $2^{(1105-1)/2} \equiv \left(\frac{2}{1105}\right) \pmod{1105}$; this is an Euler pseudoprime to base 2 (epsp-2). There are an infinite number of them.

Def. $\mathcal{E}(N) = \{a \in (\mathbb{Z}/N\mathbb{Z})^*, a^{(N-1)/2} \equiv \left(\frac{a}{N}\right) \pmod{N}\}$; $E(N) = \#\mathcal{E}(N)$.

Them. $E(N)/\varphi(N) \leq 1/2$.

Prop. $\text{Proba}(\text{"I don't know"}) = E(N)/(N-1) \leq 1/2$.

Coro. $\text{isComposite?} \in \mathbf{RP}$ (hence $\text{isPrime?} \in \mathbf{co-RP}$).

Improvement: Miller-Rabin

Idea: N being odd, write $N-1 = 2^s t$ with $s \geq 1$ and odd t .

$$a^{N-1} - 1 = (a^t - 1)(a^t + 1)(a^{2t} + 1) \cdots (a^{2^{s-1}t} + 1)$$

$$(MR_a) : a^t \equiv 1 \pmod{N} \text{ or } \exists j, 0 \leq j < s, a^{2^j t} \equiv -1 \pmod{N}.$$

Pb: $N = 2047 = 23 \times 89$ is s.t. $N-1 = 2 \times 1023$ and $2^{(N-1)/2} \equiv 1 \pmod{N}$: strong-pseudoprime to base 2 (spsp-2).

Def. $F(N) = \#\{a \in (\mathbb{Z}/N\mathbb{Z})^*, (MR_a) \text{ is satisfied}\}$.

Thm. [Monier] $F(N)/(N-1) \leq 1/4$.

Building primes?

function randomProbablePrime(b)

repeat

choose odd N at random in $[2^{b-1}, 2^b[$

until N passes k tests.

$$p_{b,k} = \text{Proba}(X = N \text{ is composite} | Y_k = N \text{ passes } k \text{ tests}) = ?$$

Rem. What we know is

$$\text{Proba}(Y_k = N \text{ passes } k \text{ tests} | X = N \text{ is composite}) \leq (1/4)^k.$$

Thm. (Burthe, 1996) $\forall b \geq 2, \forall k \geq 1, p_{b,k} \leq 4^{-k}$.

C) Application to factorization: Pollard's $p-1$

- Invented by Pollard in 1974.
- Williams: $p+1$.
- Bach and Shallit: Φ_k factoring methods.
- Shanks, Schnorr, Lenstra, etc.: quadratic forms.
- Lenstra (1985): ECM.

Rem. Almost all the ideas invented for the classical $p-1$ can be transposed to the other methods.

First phase

Idea: assume $p \mid N$ and a is prime to p . Then

$$(p \mid a^{p-1} - 1 \text{ and } p \mid N) \Rightarrow p \mid \gcd(a^{p-1} - 1, N).$$

Generalization: if R is known s.t. $p - 1 \mid R$,

$$p \mid \gcd((a^R \bmod N) - 1, N).$$

How do we find R ? Only reasonable hope is that $p - 1 \mid B!$ for some (small) B . In other words, $p - 1$ is B -smooth.

Algorithm: $R = \prod_{p^\alpha \leq B_1} p^\alpha = \text{lcm}(2, \dots, B_1)$.

Ex.

k	$b = 2^{k!} \bmod 143$	$\gcd(b - 1, 143)$
2	4	1
3	64	1
4	27	13

since $13 - 1 = 2^2 \times 3$.

Second phase: the classical one

Let $b = a^R \bmod N$ and $\gcd(b, N) = 1$.

Hyp. $p - 1 = Qs$ with $Q \mid R$ and s prime, $B_1 < s \leq B_2$.

Test: is $\gcd(b^s - 1, N) > 1$ for some s .

$s_j = j$ -th prime. In practice all $s_{j+1} - s_j$ are small (Cramer's conjecture implies $s_{j+1} - s_j \leq (\log B_2)^2$).

- Precompute $c_\delta \equiv b^\delta \bmod N$ for all possible δ (small);
- Compute next value with one multiplication
 $b^{s_{j+1}} = b^{s_j} c_{s_{j+1} - s_j} \bmod N$.

Cost: $O((\log B_2)^2) + O(\log s_1) + (\pi(B_2) - \pi(B_1))$ multiplications + $(\pi(B_2) - \pi(B_1))$ gcd's. When $B_2 \gg B_1$, $\pi(B_2)$ dominates.

Rem. We need a table of all primes $< B_2$; memory is $O(B_2)$.

Record. Nohara (66dd of $960^{119} - 1$, 2006; see <http://www.loria.fr/~zimmerma/records/Fminus1.html>).

Second phase: BSGS

Select $w \approx \sqrt{B_2}$, $v_1 = \lceil B_1/w \rceil$, $v_2 = \lceil B_2/w \rceil$.

Write our prime s as $s = vw - u$, with $0 \leq u < w$, $v_1 \leq v \leq v_2$.

Lem. $\gcd(b^s - 1, N) > 1$ iff $\gcd(b^{vw} - b^u, N) > 1$.

Algorithm:

1. Precompute $b^u \bmod N$ for all $0 \leq u < w$.
2. Precompute all $(b^w)^v$ for all $v_1 \leq v \leq v_2$.
3. For all u and all v evaluate $\gcd(b^{vw} - b^u, N)$.

Number of multiplications: $w + (v_2 - v_1) + O(\log_2 w) = O(\sqrt{B_2})$

Memory: $O(\sqrt{B_2})$.

Number of gcd: $\pi(B_2) - \pi(B_1)$.

Second phase: using fast polynomial arithmetic

Algorithm:

1. Compute $h(X) = \prod_{0 \leq u < w} (X - b^u) \in \mathbb{Z}/N\mathbb{Z}[X]$
2. Evaluate all $h((b^w)^v)$ for all $v_1 \leq v \leq v_2$.
3. Evaluate all $\gcd(h(b^{vw}), N)$.

Analysis:

Step 1: $O((\log w)M_{\text{pol}}(w))$ operations (using a product tree).

Step 2: $O((\log w)M_{\text{int}}(\log N))$ for b^w ; $v_2 - v_1$ for $(b^w)^v$; multi-point evaluation on w points takes $O((\log w)M_{\text{pol}}(w))$.

Rem. Evaluating $h(X)$ along a geometric progression of length w takes $O(w \log w)$ operations (see Montgomery-Silverman).

Total cost: $O((\log w)M_{\text{pol}}(w)) = O(B_2^{0.5+o(1)})$.

Trick: use $\gcd(u, w) = 1$ and $w = 2 \times 3 \times 5 \dots$

Program all these versions and try to factor some numbers, e.g., those of the web page.

A) General results

Thm. (characteristic) Let \mathbb{F} be a finite field.

- a) There exists a smallest $p > 1$ s.t. $p \cdot 1_{\mathbb{F}} = 0$; p is prime.
- b) The set $\{k \cdot 1_{\mathbb{F}}, 0 \leq k < p\}$ is the smallest subfield of \mathbb{F} ; it is isomorphic to \mathbb{F}_p (prime subfield of \mathbb{F}).

Thm.

$$\begin{array}{ccc} \mathbb{F} \times \mathbb{F} & \rightarrow & \mathbb{F} \\ (x, y) & \mapsto & x + y \end{array} \quad \text{and} \quad \begin{array}{ccc} \mathbb{F}_p \times \mathbb{F} & \rightarrow & \mathbb{F} \\ (a, x) & \mapsto & ax \end{array}$$

turn \mathbb{F} into a \mathbb{F}_p -vector space. If n is the dimension of this space, \mathbb{F} has p^n elements.

Thm. \mathbb{F}^\times is cyclic.

Frobenius

Thm.

$$\begin{array}{ccc} \sigma_F : \mathbb{F} & \rightarrow & \mathbb{F} \\ x & \mapsto & x^p. \end{array}$$

It is a field automorphism, i.e.

$$\sigma_F(1) = 1, \quad \sigma_F(x + y) = \sigma_F(x) + \sigma_F(y), \quad \sigma_F(xy) = \sigma_F(x)\sigma_F(y).$$

Fixed points are the elements of \mathbb{F}_p .

Proof: (hint: Lucas)

Building finite fields

Thm. (the canonical way)

Let $f(X)$ be an irreducible polynomial of degree n over \mathbb{F}_p .

Then $\mathbb{F}_p[X]/(f(X))$ is a finite field of degree n and cardinality p^n , noted \mathbb{F}_{p^n} .

You are kindly invited/strongly encouraged to attend A. Canteaut's lab on finite fields on Thursday October, 6th, from 8h45 to 10h15. See also 2-13-2 homepage for lecture notes on finite fields.

Quadratic reciprocity (1/2)

Legendre symbol: for prime odd p and $a \in \mathbb{Z}$

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } p \mid a \\ 1 & \text{if } \exists x \text{ s.t. } a \equiv x^2 \pmod{p} \\ -1 & \text{otherwise.} \end{cases}$$

Easy properties:

(i) $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$;

(ii) $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$;

(iii) $\left(\frac{a}{p}\right) = \left(\frac{a \bmod p}{p}\right)$;

(iv) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$;

Quadratic reciprocity (2/2)

Not so easy properties: (Gauss)

(v) $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$;

(vi) (Quadratic reciprocity law) p and q odd primes:

$$\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \times \frac{q-1}{2}} \left(\frac{p}{q}\right).$$

Jacobi symbol: $n \in \mathbb{Z}$, $m = \prod_{i=1}^k p_i \in \mathbb{Z}$ odd,

$$\left(\frac{n}{m}\right) = \prod_{i=1}^k \left(\frac{n}{p_i}\right).$$

Properties: same as for the Legendre symbol.

Ex. Show that $\left(\frac{n}{m}\right) = 0$ iff $\gcd(n, m) > 1$.

Example

Build \mathbb{F}_{41^2} , using a quadratic non-residue modulo 41.

$$\begin{aligned} \left(\frac{7}{41}\right) &= (-1)^{(41-1)/2 \times (7-1)/2} \left(\frac{41}{7}\right) \\ &= \left(\frac{41}{7}\right) = \left(\frac{41 \bmod 7}{7}\right) \\ &= \left(\frac{6}{7}\right) = \left(\frac{2}{7}\right)\left(\frac{3}{7}\right) = \left(\frac{3}{7}\right) = (-1)\left(\frac{7}{3}\right) \\ &= -\left(\frac{1}{3}\right) = -1 \end{aligned}$$

$$\Rightarrow \mathbf{K}_1 = \mathbb{F}_{41^2} \sim \mathbb{F}_{41}[X]/(X^2 - 7).$$

This is a vector space of dimension 2 over \mathbb{F}_{41} .

Let $\theta = \bar{X}$. All elements can be written $a + b\theta$ where a, b are in \mathbb{F}_{41} .

$\theta^2 - 7 = \bar{X}^2 - \bar{7} = 0$. We get

$$\theta^2 = 7, \theta^3 = 7\theta, \theta^4 = 8, \dots, \theta^{80} = 1,$$

so that θ does not generate \mathbf{K}^* , but $\theta + 10$ does.

Application (1/2)

Pb. Given $\left(\frac{a}{p}\right) = 1$, compute $\sqrt{a} \pmod{p}$.

Case $p \equiv 3 \pmod{4}$: $r = a^{(p+1)/4} \pmod{p}$.

Case $p \equiv 1 \pmod{4}$: find b s.t. $\Delta = b^2 - 4a$ is not a square.

$$\alpha = (-b + \sqrt{\Delta})/2 \Rightarrow \alpha^p = (-b - \sqrt{\Delta})/2 \Rightarrow \alpha\alpha^p = a$$

since $\sqrt{\Delta}^p = \left(\frac{\Delta}{p}\right)\sqrt{\Delta}$.

Let $\beta = \alpha^{(p+1)/2} \pmod{(p, X^2 + bX + a)}$. Then

$$\beta^2 = \alpha^{p+1} = a;$$

$$\beta^p = \beta(\beta^2)^{(p-1)/2} = \beta a^{(p-1)/2} = \beta$$

$\Rightarrow \beta \in \mathbb{F}_p$.

Application (2/2)

Let $a = 2 \pmod{41}$, which is a square;
 $b = 1$ is s.t. $\Delta = 1 - 4 \times 2 = -7$ which is not a square; hence
 $\mathbb{F}_{41^2} \sim \mathbb{F}_{41}[X]/(X^2 + X + 2)$.

$$\alpha = X, \quad \alpha^p = 40X + 40, \quad \alpha\alpha^p = 2.$$

$$\beta = X^{(p+1)/2} = 17, \quad 17^2 \equiv 2 \pmod{41}.$$

B) Application to primality proving

$N + 1$ **test:** (Lucas-Lehmer) For a_0 and a_1 integers, let:

$$A_N = A_N(a_0, a_1) = \mathbb{Z}/N\mathbb{Z}[T]/(T^2 + a_1T + a_0), \quad \Delta = a_1^2 - 4a_0.$$

Elements of A_N are $u + v\alpha$ with u, v dans $\mathbb{Z}/N\mathbb{Z}$, computations made using $\alpha^2 = -a_1\alpha - a_0$.

Thm. Let p be a prime $\nmid \Delta$.

- if $(\Delta/p) = -1$, then $A_p \sim \mathbb{F}_{p^2}$;
- if $(\Delta/p) = +1$, then $A_p \sim \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

Proof : If $(\Delta/p) = -1$, $T^2 + a_1T + a_0$ is irreducible, hence we recover the classical construction of \mathbb{F}_{p^2} .

If $(\Delta/p) = +1$, $T^2 + a_1T + a_0 = (T - u)(T - v)$ with $u \not\equiv v \pmod{p}$.

Therefore

$$A_p \sim (\mathbb{Z}/p\mathbb{Z})[T]/(T - u) \times (\mathbb{Z}/p\mathbb{Z})[T]/(T - v) \sim \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}. \square$$

Fundamental theorem

Thm. Let N be an odd integer. Assume that we found a_0, a_1 s.t. $\Delta = a_1^2 - 4a_0$ satisfies $(\Delta/N) = -1$. Write $N + 1 = \prod_i q_i^{\beta_i}$. Suppose we have found $\theta \in A_N = A_N(a_0, a_1)$ s.t.

$$\theta^{N+1} = 1 \text{ in } A_N,$$

and for all i :

$$\theta^{(N+1)/q_i} = u_i + v_i\alpha \text{ with } (u_i - 1, v_i, N) = 1.$$

Then N is prime.

Proof : assume N is composite and let $p \mid N$ with $p \leq \sqrt{N}$.

Reduce $A_N \pmod{p}$ towards A_p :

$$\tau = \theta \pmod{p} = (u \pmod{p}) + (v \pmod{p})\alpha.$$

We get

$$\tau^{N+1} = 1 \text{ in } A_p, \quad \tau^{(N+1)/q_i} \neq 1 \text{ in } A_p$$

which proves τ has ordre $N + 1$ in $(A_p)^*$.

Hence $N + 1 \leq \#A_p = p^2$, contradiction. \square

Remarks

- Pocklington-like theorems exist.
- Deduce from this the degree 2 pseudoprimes.
- **Lucas-Lehmer:** $M_m = 2^m - 1$ is prime iff for $L_0 = 4$, $L_{n+1} = L_n^2 - 2 \pmod{M_m}$, one has $L_{m-2} = 0$ [using $\sqrt{3}$].

\Rightarrow largest known primes, e.g., $M_{74,207,281}$ with 22, 338, 618 decimal digits (2016/01).

Lower bound (?) for primality proving algorithms:

$O((\log N)M(M_p))$ (super fast arithmetic!).

B) En route for P

- Gauss and Jacobi sums: L. Adleman, C. Pomerance, S. Rumely (1980, 1983); H. Cohen, H. W. Lenstra, Jr (1981 – 1984) ; H. Cohen, A. K. Lenstra (1982, 1987). W. Bosma & M.-P. van der Hulst (1990) ; P. Mihăilescu (1998). **deterministic** $O((\log N)^{c_1 \log \log \log N})$.
- almost **RP**: Goldwasser and Kilian using elliptic curves (1986); practical algorithm by Atkin (1986; later FM). See Smith's part.
- **RP**: Adleman and Huang using hyperelliptic curves (1986ff). See Smith's part.

Agrawal, Kayal, Saxena (AKS)

First idea: (Agrawal, Biswas – 1999)

Prop. N is prime iff $P(X) = (X + 1)^N - X^N - 1 \equiv 0 \pmod{N}$.

In practice: choose $Q(X) \in \mathbb{Z}/N\mathbb{Z}[X]$ at random of degree $O(\log N)$. If

$$(X + 1)^N \not\equiv X^N + 1 \pmod{(Q(X), N)}$$

then N is composite.

The probability of failure is bounded by $1 - 1/(4 \log N)$.

Conjecture: If N is composite, there exists $1 \leq r \leq \log N$ s.t. $P(X)$ is not divisible by $X^r - 1$ modulo N .

Agrawal, Kayal, Saxena

Thm. Let N, s be integers, r a prime number and $q = P(r - 1)$. If:

(0)

$$\binom{q-1+s}{s} > N^{2\lfloor \sqrt{r} \rfloor};$$

(i) $N \neq M^k, k > 1$;

(ii) N has no prime factor $\leq s$;

(iii) $N^{(r-1)/q} \pmod{r} \notin \{0, 1\}$;

(iv) $\forall a, 1 \leq a \leq s, (X - a)^N \equiv X^N - a \pmod{(X^r - 1, N)}$;

then N is prime.

For a proof, see FM's Bourbaki article.

What next?

- cf. D. Bernstein homepage for more on the history of improvements to the basic test; including: [H. W. Lenstra, Jr.](#) ($\tilde{O}_{\text{eff}}((\log N)^{12})$ or $\tilde{O}((\log N)^8)$), [S. David](#).
- Cleaner version of **AKS**: $\tilde{O}_{\text{eff}}((\log N)^{10.5})$ or $\tilde{O}((\log N)^{7.5})$.
- [H. W. Lenstra, C. Pomerance](#) : $\tilde{O}_{\text{eff}}((\log N)^6)$.
- [P. Berrizbeitia / Q. Cheng](#) :
Let r prime s.t. $r^\alpha \parallel N - 1, r \geq \log^2 N; 1 < a < N$ s.t.
 $a^{r^\alpha} \equiv 1 \pmod{N}, \gcd(a^{r^{\alpha-1}} - 1, N) = 1,$
 $(X + 1)^N \equiv X^N + 1 \pmod{(X^r - a, N)}$, then N is prime. Heuristic complexity would be $\tilde{O}((\log N)^4)$ for these numbers.
- [D. Bernstein, P. Mihăilescu](#): use $e \mid N^d - 1$; inject cyclotomic ideas, $\tilde{O}((\log N)^4)$.

Conclusions for primality

Which algorithm?

- **easy to understand / implement, fast:** compositeness tests;
- **fast, proven:** Jacobi;
- **fast, heuristic:** ECPP;
- **certificate:** ECPP;
- **deterministic polynomial:** AKS.

D. Bernstein has an AKS example for $2^{1024} + 643$ (13 hours on 800 MHz PC, 200 Mb memory).

To be compared to FASTECPP:

14/07/03: FM, **7000dd** with mpifastECPP.

19/08/03: J. Franke, T. Kleinjung, T. Wirth, **10000dd**.

15/10/10: FM, **25,050 dd** with mpifastECPP (2000 CPU days).

Rem. 2013: Franke et al., **30,008 dd** with combination CIDE.

V. Generic DLP

DLP: given $h \in G = \langle g \rangle$ of order N , find an integer n , $0 \leq n < N$ such that $h = g^n$.

Z) The Pohlig-Hellman reduction.

A) Enumeration; baby-steps, giant steps (adaptation as exercises).

B) RHO.

C) Nechaev-Shoup.

Z) The Pohlig-Hellman reduction

Idea: reduce the problem to the case N prime.

$$N = \prod_i p_i^{\alpha_i}$$

Solving $g^n = h$ is equivalent to knowing $n \bmod N$, i.e. $n \bmod p_i^{\alpha_i}$ for all i (chinese remainder theorem).

Idea: let $p^\alpha \parallel N$ and $m = N/p^\alpha$. Then $b = h^m$ is in the cyclic group of order p^α generated by g^m . We can find the log of b in this group, which yields $n \bmod p^\alpha$.

Cost: $O(\max(DL(p^\alpha))) = O(\max(DL(p)))$.

Consequence: for DH, N must have at least one large prime factor.

B) The RHO method

Basic model: birthday paradox

Let E be a finite set of cardinality m .

Thm. Suppose we draw uniformly n elements from E with replacement. The probability that all n elements are distinct is $\text{Proba} = \frac{1}{m} \prod_{k=1}^{n-1} (1 - \frac{k}{m})$.

Taking logarithms, and assuming $n \ll m$, we get

$$\log \text{Proba} \approx \log(n/m) - \frac{n(n-1)}{2m}.$$

\Rightarrow taking $n = O(\sqrt{m})$ will give a somewhat large value for this probability.

A very simple algorithm

Function *NaiveDL*(G, g, N, h)

Input : $G \supset \langle g \rangle$, g of order N

Output: $0 \leq n < N$, $g^n = h$

initialize a table \mathcal{L} for storing u triplets (elt of G , two ints $< N$);

repeat

draw u and v at random modulo N ;

$H \leftarrow g^u \circ h^v$;

if $\exists (H', u', v') \in \mathcal{L}$ such that $H = H'$ **then**

 // $H = g^u \circ h^v = g^{u'} \circ h^{v'}$

 // hence $n(v - v') = u' - u \pmod N$

if $v - v'$ is invertible modulo N **then**

 return $(u' - u)/(v - v') \pmod N$;

else

 store($\mathcal{L}, (H, u, v)$);

until a collision is found;

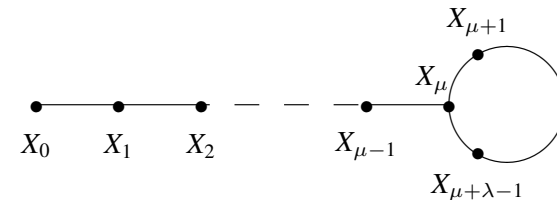
Complexity: $O(\sqrt{n} \log n)$ on average, together with a space $O(\sqrt{n})$, which is no better than BSGS.

Functional digraphs

Let $f : E \rightarrow E$ be a function on E .

Consider $X_{n+1} = f(X_n)$ for some starting point $X_0 \in E$.

The **functional digraph** of X is built with vertices X_i 's; an edge is put between X_i and X_j if $f(X_i) = X_j$.



The first part of the sequence is the set of X_i 's that are reached only once and there are μ of them.

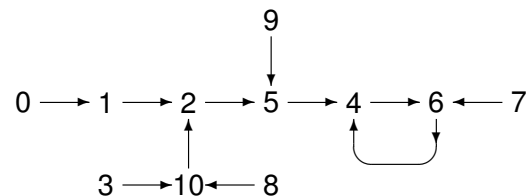
The second part forms a loop containing λ distinct elements.

Rem. λ and ν cannot be too large on average (use $n = \lambda + \mu$ in the Theorem).

Examples

1) $E = G$ finite group, $f(x) = ax$ and $x_0 = a \Rightarrow (x_n)$ purely periodic, i.e., $\mu = 0$, and $\lambda = \text{ord}_G(a)$.

2) Take $E = \mathbb{Z}/11\mathbb{Z}$ and $f : x \mapsto x^2 + 1 \pmod{11}$



Typical shape: a cycle and trees plugged on the structure.

Epackt

Goal: find λ and μ .

Prop. There exists a unique $e > 0$ (**epackt**) s.t. $\mu \leq e < \lambda + \mu$ and $X_{2e} = X_e$.

It is the smallest non-zero multiple of λ that is $\geq \mu$: if $\mu = 0$, $e = \lambda$ and if $\mu > 0$, $e = \lceil \frac{\mu}{\lambda} \rceil \lambda$.

Proof:

Function $epact(f, x_0)$

Input : A function f , a starting point x_0

Output: The epact of (x_n) defined by $x_{n+1} = f(x_n)$

$x \leftarrow x_0; y \leftarrow x_0; e \leftarrow 0;$

repeat

$e \leftarrow e + 1;$

$x \leftarrow f(x);$

$y \leftarrow f(f(y));$

until $x = y;$

return $e.$

Cost: $3e$ evaluations of f and e comparisons. For decreasing the number of evaluations, see Brent (and Montgomery).

Convenient source: Flajolet & Odlyzko (EUROCRYPT 1989).

Thm. When $m \rightarrow \infty$

$$\bar{\lambda} \sim \bar{\mu} \sim \sqrt{\frac{\pi m}{8}} \approx 0.627\sqrt{m}.$$

Thm. $\bar{e} \sim \sqrt{\frac{\pi^5 m}{288}} \approx 1.03\sqrt{m}.$

Fundamental coro. A collision is expected to be found after $O(\sqrt{m})$ computations.

Application to DL

Pollard: build a function f from G to G appearing to be random, i. e., the epact of f is $c\sqrt{N}$ for some small c .

... **Teske:**

- precompute r random elements $z_i = g^{\gamma_i} \circ h^{\delta_i}$ for $1 \leq i \leq r$ for some random exponents (say $r = 20$);
- use some hash function $\mathcal{H} : G \rightarrow \{1, \dots, r\}$;
- define $f(y) = y \circ z_{\mathcal{H}(y)}$ so that

$$x_i = g^{c_i} \circ h^{d_i},$$

where (c_i) and (d_i) are two integer sequences.

Ex. if G contains integers, we may simply use $\mathcal{H}(x) = 1 + (x \bmod r)$.

Application to DL (cont'd)

When e is found:

$$g^{c_{2e}} \circ h^{d_{2e}} = g^{c_e} \circ h^{d_e}$$

or

$$g^{c_{2e}-c_e} = h^{d_e-d_{2e}}$$

i.e.,

$$n(c_{2e} - c_e) \equiv (d_e - d_{2e}) \pmod{N}.$$

Function $Iterate(G, N, \mathcal{H}, (z_i, \gamma_i, \delta_i), x, u_x, v_x)$

Input : $\mathcal{H} : G \rightarrow \{1, \dots, r\}$; $(z_i)_{1 \leq i \leq r}$ random powers $z_i = g^{\gamma_i} \circ h^{\delta_i}$ of G ; $x = g^{u_x} h^{v_x}$

Output: $f(x, u_x, v_x) = (w, u_w, v_w)$ s.t. $w = g^{u_w} \circ h^{v_w}$
 $i \leftarrow \mathcal{H}(x);$

return $(x \circ z_i, u_x + \gamma_i \pmod{N}, v_x + \delta_i \pmod{N}).$

The algorithm

Function $RHO(G, g, N, h, \mathcal{H}, (z_i, \gamma_i, \delta_i))$

Input : $\mathcal{H} : G \rightarrow \{1, \dots, r\}$; $(z_i)_{1 \leq i \leq r}$ random powers $z_i = g^{\gamma_i} \circ h^{\delta_i}$ of G

Output: $0 \leq n < N, g^n = h$

if $h = 1_G$ **then**

└ **return** 0

$x \leftarrow h; u_x \leftarrow 0; v_x \leftarrow 1;$

$y \leftarrow x; u_y \leftarrow u_x; v_y \leftarrow v_x;$

repeat

┌ // invariant: $x = g^{u_x} \circ h^{v_x}, y = g^{u_y} \circ h^{v_y}$

┌ $(x, u_x, v_x) \leftarrow \text{literate}(G, N, \mathcal{H}, (z_i, \gamma_i, \delta_i), x, u_x, v_x);$

┌ $(y, u_y, v_y) \leftarrow \text{literate}(G, N, \mathcal{H}, (z_i, \gamma_i, \delta_i), y, u_y, v_y);$

┌ $(y, u_y, v_y) \leftarrow \text{literate}(G, N, \mathcal{H}, (z_i, \gamma_i, \delta_i), y, u_y, v_y);$

until $x = y;$

// $g^{u_x} \circ h^{v_x} = g^{u_y} \circ h^{v_y}$

if $v_x - v_y$ is invertible modulo N **then**

└ **return** $(u_y - u_x) / (v_x - v_y) \pmod{N};$

else

└ **return** Failure.

A variant for factoring integers

Pollard's idea: suppose $p \mid N$ and we have a random $f \pmod{N}$ s.t. $f \pmod{p}$ is "random".

Function $RHO(N)$

Input : N an integer

Output: a factor of N

$x \leftarrow 1; y \leftarrow 1; g \leftarrow 1;$

while $g = 1$ **do**

┌ $x \leftarrow f(x, N);$

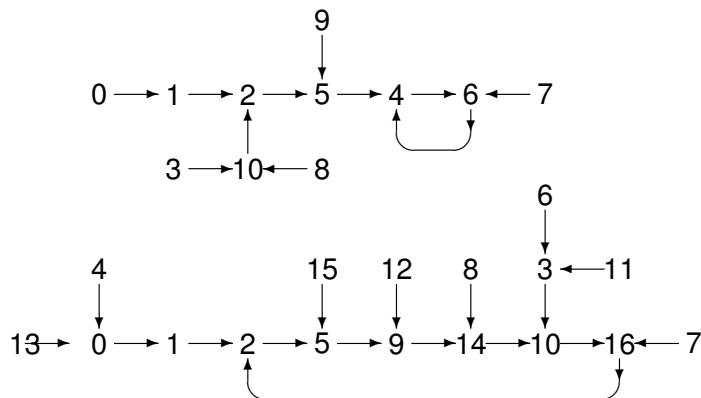
┌ $y \leftarrow f(f(y, N), N);$

┌ $g \leftarrow \text{gcd}(x - y, N);$

└ **return** $g.$

Pollard's RHO: factoring $N = 187$

i	x_i	y_i	$\text{gcd}(x_i - y_i, N)$
1	1	2	1
2	2	26	1
3	5	180	1
4	26	70	11



C) Nechaev/Shoup

Thm. Any generic group DL algorithm requires $\Theta(\sqrt{N})$ group operations.

Rough idea: given DL's for h_1, h_2, \dots, h_k , we can only build new DL's for $O(k^2)$ elements of G . To cover G , we need $k \approx \sqrt{N}$.

Take home messages

To get a feeling, program everything for the simple case of $(\mathbb{Z}/p\mathbb{Z})^*$.

To have a better than square-root algorithm for DL, you need specific ideas for specific groups. \Rightarrow [Barbulescu's part](#)

Many crypto problems of size n may have solution algorithms in $O(\sqrt{n})$ (time and/or space; deterministic or probabilistic).