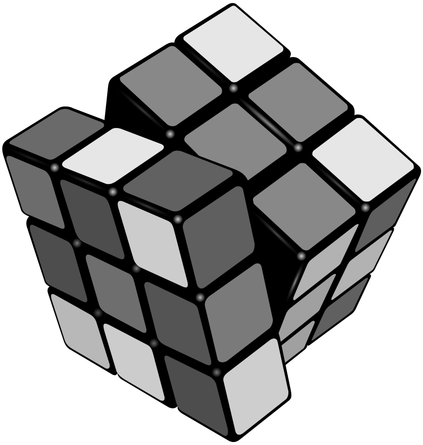
Autumn School of the Department of Algebra

Ústupky, November 24–27, 2016

BOOK OF ABSTRACTS



Cover image courtesy of Wikipedia.

Contents

British Elevator – Part I

Jan Butora

In this talk we'll focus on some concepts needed to understand one of the easy algorithms for computing discrete logarithm on elliptic curves of certain properties. Firstly we introduce p-adic numbers, their representation and some of their properties. In the second part we take a brief introduction into formal groups and formal logarithm.

1. p-adic numbers

Throughout the talk, we'll always assume p is prime and fixed and R is a ring.

Definition 1 (p-adic valuation)**.** If $0 \neq x \in \mathbb{Z}$, the *p-adic valuation* of x is

$$v_p(x) = \max\{r : p^r \mid x\} \geq 0$$

For $a/b \in \mathbb{Q}$, the *p-adic valuation* of a/b

$$v_p\left(\frac{a}{b}\right) = v_p(a) - v_p(b)$$

We also introduce the convention that $v_p(0) = \infty$.

Lemma 2. *If $x, y \in \mathbb{Q}$, the v_p has the following properties:*

(1) $v_p(x) = \infty$ if and only if $x = 0$;
(2) $v_p(xy) = v_p(x) + v_p(y)$;
(3) $v_p(x + y) \geq min\{v_p(x), v_p(y)\}$ with equality if $v_p(x) \neq v_p(y)$.

Definition 3 (p-adic norm)**.** For $x \in \mathbb{Q}$, let *the p-adic norm* of x be given by

$$|x|_p = \begin{cases} p^{-v_p(x)} & \text{if } x \neq 0, \\ p^{-\infty} = 0 & \text{if } x = 0. \end{cases}$$

Now let $(a_n)_{n \geq 1}$ be a sequence of elements in R, a ring with norm $|\cdot|_p$. We define the limit of a sequence and Cauhy sequences in same way as in real numbers, using p-adic norm instead of absolute value.

Definition 4 (Complete ring)**.** A ring with norm $|\cdot|_p$ is *complete with respect to the norm* $|\cdot|_p$ if every Cauchy sequence has a limit in R with respect to $|\cdot|_p$. Denote $\hat{R}$ the *completion of R with respect to the norm* $|\cdot|_p$.

Definition 5 (p-adic numbers)**.** The ring of *p-adic numbers* is the completion $\hat{\mathbb{Q}}$ of $\mathbb{Q}$ with respect to $|\cdot|_p$; we will denote it $\mathbb{Q}_p$.

Definition 6 (p-adic integers)**.** The unit ball about $0 \in \mathbb{Q}_p$ is the set of *p-adic integers*,

$$\mathbb{Z}_p = \{\alpha \in \mathbb{Q}_p : |\alpha|_p \leq 1\} = \{\alpha \in \mathbb{Q}_p : v_p(\alpha) \geq 0\}.$$

Definition 7 (Formal group)**.** A (one-dimensional) *formal group* $\mathscr{F}$ over a commutative ring R is a power series $F(X,Y) \in R[[X,Y]]$, such that

(1) $F(X,Y) = X + Y +$ terms of higher degree
(2) $F(X, F(Y,Z)) = F(F(X,Y),Z)$ (associativity)
(3) $F(X,Y) = F(Y,X)$ (commutativity)
(4) $\exists!$ power series $i(T) \in R[[T]]$, such that $F(T, i(T)) = 0$ (inverse)
(5) $F(X,0) = X$ and $F(0,Y) = Y$

We call $F(X,Y)$ the *formal group law.*

Definition 8. Let R be a complete local ring with maximal ideal $\mathscr{M}$ and $\mathscr{F}$ a formal group defined over R, with formal group law $F(X,Y)$. The *group associated to* $\mathscr{F}/R$, denoted by $\mathscr{F}(\mathscr{M})$, is the set $\mathscr{M}$ endowed with the group operations.

$$x \oplus_{\mathscr{F}} y = F(x,y) \quad \text{(addition)} \quad \text{for } x, y \in \mathscr{M},$$

$$\ominus_{\mathscr{F}} x = i(x) \quad \text{(inversion)} \quad \text{for } x \in \mathscr{M}.$$

Definition 9. The *formal additive group*, denoted by $\hat{\mathbb{G}}_a$, is defined by

$$F(X,Y) = X + Y.$$

Definition 10. An *invariant differential* on a formal group $\mathscr{F}/R$ is a differential form

$$\omega(T) = P(T)dT \in R[[T]]dT$$

satisfying

$$\omega \circ F(T,S) = \omega(T).$$

Writing this out, $\omega(T) = P(T)dT$ is an invariant differential if it satisfies

$$P(F(T,S))F_X(T,S) = P(T)dT,$$

where $F_X(T,S)$ is the partial derivative of F with respect to its first variable. An invariant differential is said to be *normalized* if $P(0) = 1$.

Definition 11 (Formal logarithm)**.** Let R be a torsion-free[1] ring, let $K = R \otimes \mathbb{Q}$, let $\mathscr{F}/R$ be a formal group, and let

$$\omega(T) = (1 + c_1 T + c_2 T^2 + \cdots)dT$$

be the normalized invariant differential on $\mathscr{F}/R$. The *formal logarithm of* $\mathscr{F}/R$ is the power series

$$\log_{\mathscr{F}}(T) = \int \omega(T) = T + \frac{c_1}{2}T^2 + \frac{c_2}{3}T^3 + \cdots \in K[[T]].$$

Proposition 12. *Let R be a torsion-free ring and let $\mathscr{F}/R$ be a formal group. Then*

$$\log_{\mathscr{F}} : \mathscr{F} \to \hat{\mathbb{G}}_a$$

is an isomorphism of formal groups over $K = R \otimes \mathbb{Q}$.

[1] The assumption that R has no torsion elements means that if $n \in \mathbb{Z}$ and $\alpha \in R$ satisfy $n\alpha = 0$, then either $n = 0$ or $\alpha = 0$. Equivalently, the natural map $R \to K = R \otimes \mathbb{Q}$ is an injection.

British Elevator – Part II

Tomáš Sladovník

This lecture will continue in Jan's talk about p-adic numbers, formal groups and formal logarithm. In the first half we will continue in background preparation. We will talk about arithmetic on elliptic curves, mainly we will focus on subgroups of an elliptic curve over the field of p-adic numbers, and reduction modulo p. In the second half we will construct linear algorithm for discrete logarithm on a special type of elliptic curve, which has trace of Frobenius over $\mathbb{Z}_p$ equal 1.

1. Elliptic curves

Definition 1 (Projective space)**.** Let K be a field and $n \in \mathbb{N}$. The projective n-space over K, denoted by $\mathbb{P}^n(K)$, is the set of nonzero vectors in K^{n+1}.

$$\mathbb{P}^n(K) = \{\langle v \rangle \mid v \in K^{n+1} \setminus \{o\}\}$$

In our case we'll work with the field $\mathbb{Z}_p$ where p is a fixed prime number greater than 3.

Definition 2. The set of points of an elliptic curve over field K, denoted by $E(K)$, is the set of solutions of the cubic equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

in $\mathbb{P}^2(K)$. The equation can be reduced to the form $y^2 = x^3 + Ax + B$ and the solutions of

$$F(x, y, z) = x^3 + Axz^2 + Bz^3 - y^2z$$

are points $(x : y : 1)$, where (x, y) is a solution of cubic equation and the point at infinity $\mathcal{O} = (0 : 1 : 0)$.

Definition 3. The group law on $E(\mathbb{Z}_p)$ for points $P, Q \in E(\mathbb{Z}_p)$ is defined by $\mathcal{O}$ and the chord-tangent law of composition PQ with relation $P + Q = \mathcal{O}(PQ)$. By group of points of an elliptic curve we mean an additive group

$$(E(\mathbb{Z}_p), +, -, \mathcal{O}).$$

In our case we will work with nonsingular elliptic curve in the form

$$E : y^2 = x^3 + Ax + B,$$

where $A, B \in \mathbb{Z}_p$ and discriminant $\Delta = -16(4A^3 + 27B^2) \neq 0$.

2. Expansion Around $\mathcal{O}$

In the above described elliptic curve substitute

$$z = -\tfrac{x}{y} \text{ and } w = -\tfrac{1}{y}, \quad \text{in other words} \quad x = \tfrac{z}{w} \text{ and } y = -\tfrac{1}{w},$$

the $\mathcal{O}$ is now in $(0, 0)$, because $(x : y : z) \mapsto (x : z : -y)$ and the curve has transformed to the form

$$w = z^3 + Azw^2 + Bw^3.$$

3. E_n

Definition 4 (Reduction modulo p)**.** Reduction modulo p is defined as the mapping

$$\begin{aligned} \pi : \widehat{\mathbb{Z}}_p &\to \mathbb{Z}_p \\ x_0 + x_1 p + x_2 p^2 + \cdots &\mapsto x_0, \end{aligned}$$

where $\widehat{\mathbb{Z}}_p$ is the set of p-adic integers.

Definition 5 (Sets E_n)**.** Let $E(\mathbb{Q}_p)$ be a set of points on an elliptic curve E over a field of p-adic numbers and $n \in \mathbb{N}$ then

$$E_n(\mathbb{Q}_p) = \{P \in E(\mathbb{Q}_p) : v_p(x(P)) \leqslant -2n\} \cup \{\mathcal{O}\},$$

where $P = (x_P : y_P : z_P)$ and $x(P) = x_P$. For nonsingular curve is

$$E_0(\mathbb{Q}_p) = E(\mathbb{Q}_p).$$

Theorem 6. *For all $n \in \mathbb{N}$: $E_n(\mathbb{Q}_p)$ is a subgroup of $E(\mathbb{Q}_p)$.*

Theorem 7. *For all $n \in \mathbb{N}$: $E_n(\mathbb{Q}_p)/E_{n+1}(\mathbb{Q}_p) \cong \mathbb{Z}_p^+$.*

Persistent Homology – Part I

Peter Kálnai

In our session we present persistent homology as a mathematical formalism which extracts topological information from samples of a geometric object, in particular finite sets of points equipped with a distance function, so called *point clouds.* It leads to a large number of applications in data analysis when methods like classification, recognition, parametrisation or clustering are of interest. The method leads to qualitative knowledge about data sets, while quantitative values provided by various distances are ignored. This is appropriate in case when there is no particular metrics justified or coordinates of data samples are not natural, i.e. they carry no intrinsic meaning.

Moreover, we show that applied topological methods can produce a kind of visualisation of data sets, not by embedding them in an Euclidean space but rather by generating their representation in a form of a so called *barcodes.*

1. Algebraic Topology

Definition 1. Let K be a set and for all $v \in K$, let the singleton $\{v\}$ be called a *vertex* of K. Let $\mathcal{S}$ be collection of subsets of K. A subset of a set in $\mathcal{S}$ is called a *face.* A *simplicial complex* $(K, \mathcal{S})$ is the set K with a collection $\mathcal{S}$ that contains all vertices and all faces. An element σ of the collection $\mathcal{S}$ is called a *k-simplex* if the cardinality of the set σ is $k+1$.

Definition 2. The *kth chain group* of a simplicial complex $(K, \mathcal{S})$ is the free abelian group on its set of oriented k-simplices. An element of this group is called a *k-chain.*

The *boundary operator* $\delta_k : C_k \to C_{k-1}$ is a map acting on a k-simplex $\sigma = [v_0, \dots, v_k]$ as follows:

$$\delta_k(\sigma) = \sum_{i=0}^{k} (-1)^i [v_0, v_1, \dots, \widehat{v_j}, \dots, v_k]$$

where the hat over a vertex indicates that it was omitted from the sequence. The map δ_k is $\mathbb{Z}$-linearly extended to all simplicial complexes.

A *chain complex* is a sequence of chain groups connected with boundary operators. There are two associated subgroup with a chain complex:

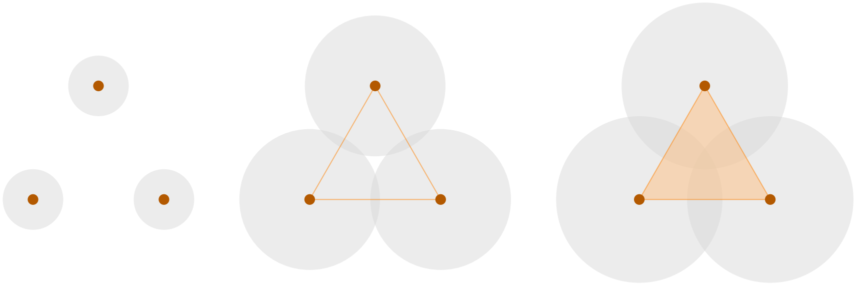
- the *cycle group* $Z_k := \ker \delta_k$
- the *boundary group* $B_k := \delta_{k+1}(C_{k+1})$
- the *kth homology group* $H_k := Z_k / B_k$

A simplicial complex may be viewed as a union of polytopes in $\mathbb{R}^{|K|}$, where the polytopes are formed from the standard basis vectors that are in bijective correspondence with the vertices of the simplicial complex.

Definition 3. Let (X, d) denote a metric space and let $B_r(x)$ denote an open d-ball centered at the point $x \in X$ with radius r. Let $X_0 := \{x_0, x_1, \dots, x_l\}$ be a point cloud. We can form a union $B_r = \cup_{i=0}^{l} B_r(x_l)$ of balls aroud the point cloud.

The *Čech complex* for the set of balls $B_r(x_i)$, $i = 0, \dots, l$, denoted by $C(X, r)$ is the simplicial complex whose vertex set consists of singletons from X_0 and whose k-simplicis correspond to $k+1$-balls with non-empty intersection.

The *Vietoris-Rips complex* for (X, d) parametrised by r, denoted by $VR(X, r)$ is the simplicial complex whose vertex set is X, and where $\{x_0, x_1, \ldots, x_k\}$ spans a k-simplex if and only if $d(x_i, x_j) \leq r$ for all $0 \leq i, j \leq k$.



Lemma 4. *For any finite point cloud X_0 in the $\mathbb{R}^d$, for any parameter $r \geq 0$, $C_r(X_0) \subseteq VR_{2r}(X) \subseteq C_{2r}(X_0)$*

Theorem 5 (Structure theorem of PIDs)**.** *Let D be a principal ideal domain. Let M be a finitely generated D-module. Then*

$$M \simeq D^\beta \oplus \left(\bigoplus_{i=1}^{m} D/d_i D \right)$$

where $\beta \in \mathbb{Z}$, $d_i \in D$, $i = 0, 1, \ldots, m$.

Persistent Homology – Part II

Michal Hrbek

1. Persistent modules

Definition 1. Let k be a field and $(P, <)$ a totally ordered poset with a dense countable subset. We naturally view the poset P as a category. A *(P-)persistence module* M is a functor from P to the category of k-vector spaces. We say that M is *pointwise finite-dimensional* if $M(p)$ is finite-dimensional for any $p \in P$.

Let I be an interval I in P. A simple example of a persistent module is the *interval module* corresponding to interval I defined as follows:

- $M(p) = \begin{cases} k, & p \in I \\ 0, & p \notin I \end{cases}$,
- $M(p < q) = \begin{cases} \mathrm{Id_k}, & p, q \in I \\ 0, & \text{otherwise} \notin I \end{cases}$

Theorem 2 (Carlsson, Crawley-Boevey)**.** *Under a mild finiteness conidition (which holds e.g. if M is pointwise finite-dimensional), a persistence module M is isomorphic to a direct sum of interval modules.*

General idea of the method for a point cloud $X \subseteq \mathbb{R}^d$:

- Given $\varepsilon \in \mathbb{R}$, construct a simplicial complex C_ε from the point cloud X using e.g. the Čech or the Vietoris-Rips method.
- Since the point cloud is finite, there are $0 = \varepsilon_0 < \varepsilon_1 < \cdots < \varepsilon_n < \varepsilon_{n+1} = \infty$ such that $C_{\varepsilon_j} = C_\varepsilon$ for any $\varepsilon_j < \varepsilon < \varepsilon_{j+1}$.
- Computing the homology in degree k, we obtain an $\mathbb{N}$-persistent module
$$H_k(C_{\varepsilon_1}) \to H_k(C_{\varepsilon_2}) \to \cdots \to H_k(C_{\varepsilon_n}) \to \cdots,$$
where the maps are induced by inclusions $C_{\varepsilon_j} \to C_{\varepsilon_{j+1}}$.
- By Carlsson's theorem, this module decomposes into a direct sum of interval modules $\bigoplus_{i=1}^{l} M(I_i)$, where I_i is a interval of $\mathbb{R}$ of form $[\varepsilon_j, \varepsilon_{j'}]$ for some $0 \leq j < j' \leq n$.

The complete set of topological data obtained by this method can be faithfully interpreted by a collections of *barcodes*. A barcode is nothing else then a multiset of intervals of form as above. Intuitively, each interval marks a birth and death of a non-zero homology cycle in dimension k. Simple heuristic is then to interpret short intervals in barcodes as **noise** and long intervals as **topologically significant**.

Modular forms

Josef Svoboda

In this lecture, we will introduce Gelfand correspondence of compact (Hausdorf) spaces and commutative C^*-algebras and explaint the (dis)similarities with classical algebraic geometric correspondence between algebraic varietes and finitely generated reduced algebras.

1. Basic definitions

Definition 1. *Banach algebra* is an associative unital algebra $\mathcal{A}$ over $\mathbb{C}$ which is also a complete normed space such that the algebra multiplication and the norm are related by the following inequality

$$\forall x, y \in \mathcal{A} : \|xy\| \leq \|x\|\|y\|.$$

A *homomorphism* of Banach algebras $\mathcal{A}$ and $\mathcal{B}$ is a bounded linear map $\varphi : \mathcal{A} \to \mathcal{B}$ which satisfies $\phi(xy) = \phi(x)\phi(y)$ for all $x, y \in \mathcal{A}$.

Definition 2. Let $\mathcal{A}$ be a Banach algebra with the identity element e. If $x \in \mathcal{A}$ then *spectrum* $\sigma(x)$ is a set of all $\lambda \in \mathbb{C}$ such that $\lambda e - x$ is not invertible.

Definition 3. *C^*-algebra* is a Banach algebra $\mathcal{A}$ together with a map $^* : \mathcal{A} \to \mathcal{A}$ satysfying for all $x, y \in \mathcal{A}$ and $\lambda \in \mathbb{C}$ the following conditions:

- $x^{**} = x$
- $(x + y)^* = x^* + y^*$
- $(\lambda x)^* = \bar{\lambda} x^*$
- $(xy)^* = y^* x^*$
- $\|xx^*\| = \|x\|\|x^*\|$.

A *homomorphism* of C^*-algebras $\mathcal{A}$ and $\mathcal{B}$ is a homomorphism of Banach algebras $\varphi : \mathcal{A} \to \mathcal{B}$ which satisfies $\phi(x^*) = \phi(x)^*$ for all $x \in \mathcal{A}$.

Definition 4. Let $\mathcal{A}$ be a commutative Banach algebra. Then *Gelfand spectrum* $\sigma(\mathcal{A})$ is a set of nonzero homomorphisms from $\mathcal{A}$ to $\mathbb{C}$.

Note. Gelfand spectrum can be naturally endowed by a weak* topology as a subspace of the unit sphere of $\mathcal{A}^*$. With this topology, Gelfand spectrum becomes a compact topological space.

Theorem 5. *Let $\mathcal{A}$ be a Banach algebra in which every nonzero element is invertible. Then $\mathcal{A} \cong \mathbb{C}$.*

Corollary. *Gelfand spectrum is in bijection with the set $Spec_M$ of maximal ideals of algebra $\mathcal{A}$.*

Definition 6. *Gelfand transform* of an element $x \in \mathcal{A}$ is a function $\hat{x} \in C(\sigma(\mathcal{A}))$ defined by $\hat{x}(h) = h(x)$ for every homomorphism $h \in \sigma(\mathcal{A})$. The map $\hat{} : \mathcal{A} \to C(\sigma(\mathcal{A}))$ is called *Gelfand transformation* and denoted by $\Gamma_{\mathcal{A}}$.

Proposition 7. *Gelfand transformation is a homomorphism of Banach algebras. Image of $\hat{x}$ is $\sigma(x)$. If x and e generate algebra $\mathcal{A}$, then $\sigma(\mathcal{A})$ and $\sigma(x)$ are homeomorphic.*

2. Correspondence of C*-algebras and compact spaces

Let **Comp** be the category of compact spaces and continuous maps. Let **Ban** be the category of Banach algebras and homomorphisms and $\mathbf{C^*Alg}$ be the full category of all C^*-algebras. We consider contravariant functors:

$$C : \mathbf{Comp} \to \mathbf{Ban}$$
$$X \mapsto C(X)$$

which assigns to every compact topological space its algebra of continuous complex fuctions and

$$S : \mathbf{Ban} \to \mathbf{Comp}$$
$$\mathcal{A} \mapsto \sigma(\mathcal{A})$$

which assigns to every C^*-algebra its Gelfand spectrum.

Proposition 8. *The functor S is a right adjoint to the functor C, with Gelfand transform as a counit nad a natural "evaluation" homomorphism as a unit.*

Theorem 9 (Gelfand - Naimark)**.** *If $\mathcal{A}$ is a commutative C^*-algebra, then Gelfand transformation $\Gamma_{\mathcal{A}}$ is an isometric isomorphism from $\mathcal{A}$ to $C(\sigma(\mathcal{A}))$.*

Corollary. *The restriction of the functor C to $\mathbf{C^*Alg}^{op}$ and the functor S form an equivalence of categories $\mathbf{C^*Alg}^{op}$ and* **Comp***.*

Undirected loop conditions

Miroslav Olšák

Universal algebra studies various conditions for algebra classification. Particular attention is given to Maltsev conditions claiming existence of some terms satisfying given equations. It was discovered in 2010 that in the case of finite algebras, there is a weakest Malstev condition of a very special form: If a finite algebra satisfy a Malstsev condition then it contain a 6-ary term operation s satisfying $s(a, b, a, c, b, c) = s(b, a, c, a, c, b)$. We will show that the existence of s is also the weakest without finiteness assumption but among much smaller range of conditions.

Algebra is a set (universe) A provided with several operations $o_1, o_2, \ldots$, written $(A, o_1, o_2, \ldots)$. These operations can be composed into *term operations.* More precisely, *term* is a syntactically correct finite string using symbols of variables $v_1, v_2 \ldots$, operations $o_1, o_2, \ldots$ and parenthesis. *Term operation* is an operation $t_A \colon A^n \to A$ described by a term t. For any choice of variables $v_1, \ldots, v_n \in A$ the value $t_A(v_1, \ldots, v_n)$ equals the calculated value of t.

For example, in rings $(R, +, -, \cdot, 0, 1)$, terms are formal polynomials and term operations are polynomial functions. In groups, an example of a term (operation) is the Maltsev term $m(x, y, z) = (x \cdot y^{-1}) \cdot z$. Even a set (S) without any operations can be considered as an algebra. In this case, term operations are just projections, for example $\pi_2(u, v, x, y) = v$.

Absolutely free algebra (in a language Σ) over a set of generators X has as its universe the set of all terms using elements of X as variables. Operations (from Σ) act in the natural way. The *free algebra* over X modulo a set of equations $\mathcal{S}$ is a quotient of the absolutely free algebra over X, where s and t are identified if and only if $s \approx t$ is a consequence of $\mathcal{S}$. For example, the free commutative ring over two generators x, y generator is the ring of polynomials: $\mathbb{Z}[x, y]$.

(Directed) graph is a pair (V, E) where V is a set of vertices and $E \subset V^2$ is the set of oriented edges – ordered pairs (a, b) where $a, b \in V$. Consider an algebra $\mathbf{A} = (A, o_1, o_2, \ldots)$ and a directed graph (A, E) with the same universe. We say that the graph (A, E) is *compatible* with the algebra if E is a subalgebra of $\mathbf{A}^2$. In other words, for any k-ary operation o_i and any edges $(a_1, b_1), (a_2, b_2), \ldots, (a_k, b_k) \in E$ the graph contain the edge

$$(o_i(a_1, a_2, \ldots, a_k), o_i(b_1, b_2, \ldots, b_k)).$$

Loop condition is a condition for algebras of the form: The algebra possesses a term operation t satisfying the equation

$$\begin{aligned} &t(\text{variables}) \\ &= t(\text{variables}). \end{aligned}$$

The arity of t and concrete choice of variables are given by concrete loop conditions. Examples of loop condition are the existence of a commutative term c and the existence of a Maltsev term m satisfying

$$\begin{aligned} &c(x, y) \qquad\qquad &&m(x, y, y) \\ &= c(y, x), &&= m(z, z, x). \end{aligned}$$

Any group satisfies the existence of Maltsev term and any lattice satisfies the existence of commutative term.

For every loop condition, there is a graph *associated* with it. The set of vertices is the set of variables used in the equation. Edges are defined to be the columns in the equation. For example, the graph associated with the existence of a commutative term is just one both-sided edge. The oriented graph associated with the existence of Maltsev term has three vertices x, y, z and three oriented edges yx, xz, yz.

Graph homomorphism from $G = (V_G, E_G)$ to $H = (V_H, E_H)$ is a mapping $f\colon V_G \to V_H$ such that for any $(a, b) \in E_G$ the image $(f(a), f(b)) \in E_H$.

Proposition 1. *Loop conditions with isomorphic associated graphs are equivalent.*

Proposition 2. *Assume an algebra* $\mathbf{A}$ *satisfying a loop condition associated with graph* G*. Consider a graph* H *compatible with* $\mathbf{A}$*. If there is a graph homomorphism* $G \to H$ *then* H *contains a loop.*

Proposition 3. *Consider a loop conditions* C*,* D *with associated graphs*

$$G_C = (V_C, E_C), \quad G_D = (V_D, E_D)$$

respectively. Let $\mathbf{A}$ *be a free algebra over generators* V_D *modulo equation* C*. Consider the minimal supergraph of* G_D *compatible with* $\mathbf{A}$*. The graph contains a loop if and only if the condition* C *implies the condition* D*.*

Proposition 4. *Consider a loop conditions* C*,* D *with associated graphs* G_C*,* G_D *respectively. If there is a graph homomorphism* $G_C \to G_D$ *then* C *implies* D*.*

Let $G = (V, E)$ be a graph associated with a loop condition. If for each edge $(a, b) \in E$ the graph contain the reverse edge (b, a) we consider it as an undirected graph and call the loop condition undirected. For example the loop condition mentioned in introduction paragraph is the undirected loop condition associated with a triangle.

The talk will lead to following result.

Theorem 5. *There are just three different (pairwise non-equivalent) loop conditions, associated with*

(1) Bipartite grahs

(2) Non-bipartite graphs without loops

(3) Graphs containing a loop

Moreover (1) ⇒ (2) ⇒ (3) and every nontrivial (directed) loop condition imply (2).

Attacking RSA

Barbora Hudcová and Igor Eržiak

1. Introduction

In this talk, we will present various attacks on RSA which mainly focus on retrieving the secret message without factorization of the modulus N. We will introduce the low-exponent attack with related messages, Wiener's attack, Coppersmith's attack and their applications. Each topic will be accompanied by a practical example in Python code.

2. Basic notions

Definition 1 (RSA cryptosystem)**.** Let $N = pq$ be the product of two primes. Let e, d be two integers satisfying

$$ed \equiv 1 \pmod{\varphi(N)}$$

where $\varphi(N) = (p-1)(q-1)$. We call N the *RSA modulus*, e the *encryption exponent* and d the *decryption exponent*.

A message is an integer $M \in \mathbb{Z}_N^*$. To encrypt M, one computes $C \equiv M^e \pmod{N}$. To decrypt the ciphertext C, the legitimate reciever computes $C^d \pmod{N}$. Indeed, from Euler's theorem it follows that

$$C^d \equiv M^{ed} \equiv M \pmod{N}.$$

3. Low-Exponent Attack With Related Messages

Given encryptions of k messages under the same RSA public key with exponent e, together with knowledge of polynomial relation of degree δ among the messages, the goal is to recover all messages.

4. Wiener's Attack

Theorem 2 (M. Wiener)**.** *Let $N = pq$ with $q < p < 2p$. Let $d < \frac{1}{3}N^{\frac{1}{4}}$. Given public key $\langle N, e\rangle$ with $ed \equiv 1 \pmod{\varphi(N)}$, an adversary can efficiently recover d.*

Lemma 3. *Suppose that* $\mathrm{GCD}(a, b) = \mathrm{GCD}(c, d) = 1$ *and*

$$\left|\frac{a}{b} - \frac{c}{d}\right| < \frac{1}{2d^2}.$$

Then $\frac{c}{d}$ is one of the convergents of the continued fraction expansion of $\frac{a}{b}$.

Lemma 4 (LLL)**.** *Let L be a lattice spanned by $\langle u_1, \ldots, u_w \rangle$, where $u_1, \ldots, u_w \in \mathbb{R}^n$. When $\langle u_1, \ldots, u_w \rangle$ are given as input, then the LLL algorithm outputs a point $v \in L$ satisfying*

$$\|v\| \leq 2^{\frac{w}{4}} \det(L)^{\frac{1}{w}}.$$

The running time of the LLL algorithm is quartic in the length of the input.

Theorem 5 (Coppersmith)**.** *Let N be an integer and $f \in \mathbb{Z}[x]$ be a monic polynomial of degree d. Set $X = N^{1/d-\varepsilon}$ for some $\varepsilon \geq 0$. Then, given $\langle N, f \rangle$, an adversary can efficiently find all integers $|x_0| < X$ satisfying $f(x_0) \equiv 0 \pmod{N}$. The running time is dominated by the time it takes to run the LLL algorithm on a lattice of dimension $O(w)$ with $w = min(\frac{1}{\varepsilon}, log_2(N))$.*

Lemma 6. *Let $h(x) \in \mathbb{Z}[x]$ be a polynomial of degree d, and let X be a positive integer. Suppose $\|h(xX)\| < \frac{N}{\sqrt{d}}$. If $|x_0| < X$ satisfies $h(x_0) \equiv 0 \pmod{N}$ then $h(x_0) = 0$ holds over the integers.*

Theorem 7 (Håstad)**.** *Let $N_1, \ldots, N_k$ be pairwise relatively prime integers, and set $N_{min} = min_i(N_i)$. Let $g_i \in Z_{N_i}[x]$ be k polynomials of maximum degree d. Suppose there exists a unique $M < N_{min}$ satisfying*

$$g_i(M) \equiv 0 \pmod{N_i} \quad \textit{for all } i = 1, \ldots, k.$$

Under the assumption that $k > d$, one can efficiently find M given $\langle N_i, g_i \rangle_{i=1}^{k}$.

Hidden Field Equations

Adolf Středa

Hidden Field Equations (HFE) is a public key cryptosystem proposed by Patarin back in 1996. It is a part of a larger group of cryptosystems based on an MQ-problem – a problem of finding solutions to Multivariate Quadratic equations.

The basic HFE cryptosystem was broken by a wide range of attacks – ranging from simple linear algebra techniques to Gröbner bases. Thus it was necessary to introduce small changes to the HFE cryptosystems giving us variants of HFE such as HFEm, HFE-, HFE$\perp$.

1. MQ-problem and HFE

Definition 1. Let $p_1, \ldots, p_m$ be a system of $m \in \mathbb{N}$ polynomials in $n \in \mathbb{N}$ variables over a field $\mathbb{F}$:

$$p_k(x, \ldots, x_n) = \sum_{i,j=1}^{n} \alpha_{k,i,j} x_i x_j + \sum_{i=1}^{n} \beta_{k,i} x_i + \gamma_k$$

$$\alpha_{k,i,j}, \beta_{k,j}, \gamma_k \in \mathbb{F} \text{ for } 1 \leq i,j \leq n \text{ and } 1 \leq k \leq m$$

Given an arbitrary vector $\vec{y} = (y_1, \ldots, y_m) \in \mathbb{F}^m$ we denote a problem of solving

$$y_k = p_k(x_1, \ldots, x_n) \text{ for every } 1 \leq k \leq m$$

as the MQ-problem.

Lemma 2. *Let $\mathbb{F} \leq \mathbb{E}$ be a field extension of a degree $n \in \mathbb{N}$. Then the carrier set of $\mathbb{E}$ with an addition and a multiplication by an element from $\mathbb{F}$ is isomorphic to the vector space $\mathbb{F}^n$. Let us denote it by $\mathbb{E}_{\mathbb{F}}$.*

Definition 3. Let $\mathbb{F}_q$ be a finite field with q elements, $\mathbb{E}$ its algebraic extension of a degree $n \in \mathbb{N}$ and let ψ be an isomorphism, $\psi : \mathbb{E} \to \mathbb{F}^n$, from the preceeding lemma. Then a polynomial vector $\mathcal{P}$ is in a *HFE-shape* if there exists a polynomial

$$P(X) = \sum_{i,j=0}^{d} A_{i,j} X^{q^i + q^j} + \sum_{i=0}^{d} B_i X^{q^i} + C, \; A_{i,j}, B_i, C \in \mathbb{E}, \; X \in \mathbb{E}$$

such that $\mathcal{P} = \psi \circ P \circ \psi^{-1}, d \in \mathbb{N}$. The polynomial P is called the *HFE polynomial*, terms $A_{i,j} X^{q^i + q^j}$ are called quadratic terms, $B_i X^{q^i}$ are linear terms and C is a constant term of the HFE polynomial.

2. HFE Cryptosystem

Since a HFE cryptosystem is not required to be bijective, we might need to add some redundancy to a plaintext in order to select the right plaintext from the affine subspace of all possible pre-images of given a ciphertext with a sufficiently high probability. As error correcting codes give too much information to the attacker cryptographically secure hash functions are preferred.

$$\begin{tikzcd}
\text{input} = (x_1, \ldots, x_n) \arrow[d] & \\
\vec{x} \arrow[d, "\text{private: } S"'] \arrow[dr] & \\
\vec{x'} \arrow[d, "\text{private: } P"'] & \text{public: } \mathcal{P} \arrow[ddl] \\
y' \arrow[d, "\text{private: } T"'] & \\
\text{output} = (y_1, \ldots, y_m) &
\end{tikzcd}$$

FIGURE 1. HFE Encryption

$$\begin{tikzcd}
\text{input} = (y_1, \ldots, y_m) \arrow[d] \\
\vec{y} \arrow[d, "\text{private: } T"'] \\
\vec{y'} \arrow[d, "\text{private: } P"'] \\
x' \arrow[d, "\text{private: } S"'] \\
\text{output} = (x_1, \ldots, x_n) = (M||h(M))
\end{tikzcd}$$

FIGURE 2. HFE Decryption

3. HFE MODIFICATIONS

- HFE$\perp$ – two affine transformations, multiple HFE polynomials (in parallel)
- HFEm – we forget some coordinates from the first transformation's output
- HFE+ – a projection of an input into a vector space of a smaller dimension
- HFEs – using sparse polynomials for the secret key