1 DL-systems and orders

1.1 Ideal class groups of orders

Remark:
Everything could be done much more general, and for some (few) theoretical and (even fewer) practical considerations this has to be done.

Let O be a (commutative) ring with unit 1 without zero divisors.

Two ideals [1] A, B of O different from 0 can be multiplied:

$$A \cdot B = \{\Sigma a_i \cdot b_i; a_i \in A, b_i \in B\}.$$

Clearly $\cdot$ is associative. How to compute A^k with
a numeration?

In general this will be not possible.
Here are some minimal assumptions:

I) O is **noetherian**:
Every A is a finitely generated $O-$module.
A generating system of the product of two ideals can be computed in finitely many steps from generators of the factors.

But these systems become longer and longer.
II)O can be embedded into a
finitely generated algebra $\tilde{O}$
over an **euclidean** ring $\mathcal{B}$
such that the transition

$$A \mapsto A \cdot \tilde{O}$$

preserves "enough" information.
Then ideals A have a **base** over $\mathcal{B}$ (as $\tilde{O}$-modules), and by linear algebra over

[1] $A \subset O$ is an ideal of O if it is an $O-$module

B one can compute a base in products of ideals.

But there are **infinitely many** possible choices of bases. So assume
III) There is a canonical basis for each ideal and $\mathcal{B}$ has a numeration. Then one can numerate ideals in O.
Severe **disadvantages:**
The system is much too large.
It is insecure.
We have infinite sets.
(We have no group structure.)

Advantage and disadvantage:
We are near to the arithmetic of $\mathcal{B}$ and we can compute with ideals if we can compute in $\mathcal{B}$. Abstract Algebraic Geometry resp.
Commutative Algebra tells us:
There are more reasonable objects than ideals (= rank-1-projective modules) over O:

Isomorphy classes of projective rank-1-modules
or, in fancy language,

$Pic(O)$

and factor- resp. subgroups.
Definition:
Let A_1, A_1 be two $O-$modules in
$Quot(O)$.
$A_1 \sim A_2$ if there is an element
$f \in Quot(O)^*$ with

$$A_1 = f \cdot A_2.$$

Let A be an ideal of O:
A is invertible iff there is an ideal $\tilde{A}$ of O such that

$$A \cdot \tilde{A} \sim O.$$

$Pic(0)$ is the set of equivalence classes of invertible ideals of O, it is an abelian group.

Try $Pic(O)$ as groups into which $\mathbb{Z}/p$ is to be embedded.

Immediate problem: The equivalence classes contain infinitely many ideals. How to describe the elements in $Pic(O)$ for the computer?

So

1. Find a distinguished element in each class (resp. a finite (small) subset of such elements).
2. or: Find "coordinates" and addition formulas directly for elements of $Pic(O)$.

We need:

I)There has to be a very fast algorithm to find these distinguished elements. Possible if

- we have "reduction algorithms", or

- we can use the geometric background of $Pic(O)$ which leads to **group schemes resp. abelian varieties** (link to the first lecture.

Most interesting cases are those for which both methods can be used!

II)We want to embed $\mathbb{Z}/p$ into $Pic(O)$ in a bit-efficient way:
We need

- a fast method for the computation of the order of $Pic(O)$
- (at least) a heuristic that with reasonable probability this order is almost a prime.

III) Discuss and, above all, **exclude attacks.**

"Generic attack" for DL-systems based on $Pic(O)$:

We have distinguished ideals: Prime ideals.

We have the arithmetic structure of $\mathcal{B}$.

Since we have to be able to define reduced elements (i.e. ideals) in classes we have in all known cases a “size” of classes which behaves reasonable with respect to addition.
This cries for ... **Index-Calculus**.

Principle:
We work in a group G .
Find a “factor base” consisting of relatively few elements and compute G as a $\mathbb{Z}-$module given by the free abelian group generated by the base elements modulo relations.
Prove that with reasonable high probability every element of G can be written (fast and explicitly) as a sum of elements in the factor base. The important task in this method is to balance the number of elements in the factor base to make the linear algebra over $\mathbb{Z}$ manageable and to “ guarantee” smoothness of enough elements with respect to this base.

The expected complexity of this attack is **subexponential**, i.e estimated by

$$L_N(\alpha, c) := exp(c(logN)^\alpha(loglogN)^{1-\alpha})$$

mit $0 < \alpha < 1$ und $c > 0$ for a number N closely related to $\mid G \mid$. Digression: Factorization of numbers

1.2 Existing Systems

What is used today?
Only two examples:

- $\mathcal{B} = \mathbb{Z}$, and O is an order or a localization of an order in a number field
- $\mathcal{B} = \mathbb{F}_p[X]$, and O is the ring of holomorphic functions of a curve defined over a finite extension field of $\mathbb{F}_p$.

1.2.1 Number field case

Orders O in number fields were proposed very early in the history of public key cryptography (Buchmann-
Williams 1988).
We restrict ourselves to the ring of integers O_K of $\mathbb{Z}$ in number fields K.
O_K is a Dedekind domain, its class group $Pic(O_K)$ is finite.
The size of ideals is given by their norm.
The **Theorem of Minkowski** states that in every ideal class there are ideals of "small" norm depending on

$$g_K := 1/2c_K \cdot log \mid \Delta_K \mid$$

(Δ_K the discriminant of $O_K/\mathbb{Z}$), c_K depending on the real and complex embeddings of K.

The background is the "Geometry of numbers" (Minkowski).
By lattice techniques it is possible to compute ideals of small norms in classes, and in these ideals one finds "small" bases.

Most difficult part: To compute the order of $Pic(O_K)$:
Uses analytic methods (L-series) in connection with most powerful tools from computational number theory.

There is a (probabilistic) estimate:
The order of $Pic(O_K)$ behaves like $exp(g_K)$.
Disadvantage: For given g there are not many fields, and to have $Pic(O_K)$ large the genus of K has to be large.

The parameter "genus" can be splitted into two components:
$n := [K : \mathbb{Q}]$ and ramification locus of $K/\mathbb{Q}$.

If n is large the arithmetic in O_K is complicated (fundamental units, lattice dimension ...)

Most practical example :
K is an imaginary quadratic field of discriminant $-D$.
So $K = \mathbb{Q}(\sqrt{-D}$. The expected size of $Pic(O)$ is $\approx \sqrt{D}$.

Theory of Gauß:
$Pic(O_K)$ corresponds to classes of
binary quadratic forms with discriminant D.

Multiplication of ideals corresponds to composition of quadratic forms.
Reduction of ideals corresponds to the (unique) reduction of quadratic forms:
In each class we find (by using Euclid's algorithm) a uniquely determined **reduced** quadratic form

$$aX^2 + 2bXY + cY^2$$

with $ac - b^2 = D$, $-a/2 < b \leq a/2, a \leq c$ and $0 \leq b \leq a/2$ if $a = c$.

The great disadvantage:
The index-calculus-attack works very efficiently:
(Under GRH:) The complexity to compute the DL in $Pic(O_K)$ is

$$O(L_D(1/2, \sqrt{2} + o(1))).$$

1.3 The geometric case

$\mathcal{B} = \mathbb{F}_p[X]$, and O is the ring of holomorphic functions of a curve defined over a finite extension field $\mathbb{F}_q$ of $\mathbb{F}_p$.
Intrinsically behind this situation is a regular projective absolutely irreducible curve C defined over $\mathbb{F}_q$ whose field of meromorphic functions $F(C)$ is given by $Quot(O)$.

C is the desingularisation of the projective closure of the curve corresponding to O.

This relates $Pic(O)$ closely with the points of the Jacobian variety J_C of C and explains the role of abelian varieties in crypto systems used today.
Singularities
We assume that O is not integrally closed.
The generalized Jacobian variety of C_p is an extension of J_C by linear groups.
Examples:

1. $Pic(\mathbb{F}_q[X,Y]/(Y^2 - X^3)$ corresponds to the additive group.
2. $Pic(\mathbb{F}_q[X,Y]/(Y^2 + XY - X^3)$
   corresponds to G_m
   and (for a non-square d)
3. $Pic(\mathbb{F}_q[X,Y]/(Y^2 + dXY - X^3)$
   corresponds to a non split one-dimensional torus.
4. More generally we apply scalar restriction (se next lecture) to $G_m/\mathbb{F}_q$ and get higher dimension tori.
   Example:
   XTR uses an irreducible two-dimensional piece of the scalar restriction of $G_m/\mathbb{F}_{q^6}$ to $\mathbb{F}_q$.
   Though there is an algebraic group (torus) in the background the system XTR seems not to use it: It uses traces of elements instead of elements in the multiplicative group of of extension fields.

1.3.1 Work of Rubin-Silverberg

To understand what is going on Silverberg and Rubin analyse rational parametrisations of (non-)split tori, are able to explain related systems like LUC and give a new system CEILIDH.
In addition they come to interesting questions (conjectures) about tori (Vroskresenskii).
They also show limits of the method.

1.3.2 Security?

We can get tori by two different methods: By scalar restriction and by the Generalized Jacobian of curves of **geometric** genus 0 and **arithmetic** genus larger than 0.

Question:
Can this structure be used (as in the case of elliptic curves, see below) for attacks?

Curves without singularities
The corresponding curve C_a is an affine part of $C_p = C$.
The inclusion

$$\mathbb{F}_q[X] \to O$$

corresponds to a morphism

$$C_O \to \mathbb{A}^1$$

which extends to a map

$$\pi : C \to \mathbb{P}^1$$

where $\mathbb{P}^1 = \mathbb{A}^1 \cup \{\infty\}$. The canonical map
$\phi : J_C(\mathbb{F}_q) \to Pic(O)$
is surjective but not always injective:
Its kernel is generated by formal combinations of degree 0 of points in $\pi^{-1}(\infty)$.
More precisely: $\mathbb{F}_q$−rational divisors of C are formal sums of points (over $\bar{\mathbb{F}}_q$) of C which are Galois invariant.
Two divisors are in the same class iff their difference consists of the zeroes and poles (with multiplicity) of a function on C.
The points of J_C are the divisor classes of degree 0 of C.
The theorem of Riemann-Roch implies that

$$(C \times \ldots \times C)/S_g \quad (g = \text{genus}(C),$$
$$S_g \text{ the symmetric group in } g \text{ letters})$$

is birationally isomorphic to J_C:

We find a representative D' in divisor classes c of the form
$D' = D - g\,P_\infty$ with $D = \Sigma_{i=1,\cdots g}\, a_i P_i$ with $a_i \geq 0$. Now map
$c \mapsto [\Pi_{P_i \in C_O}\, M_{P_i}^{a_i}]$.

Most interesting case: The kernel of ϕ is trivial.
Then we can use the ideal interpretation for computations and the abelian varieties for the structural background:

- Addition is done by ideal multiplication

- Reduction is done by Riemann-Roch theorem (replacing Minkowski's theorem in number field) on curves

but
the computation of the order of $Pic(O)$ and the construction of suitable curves is done by using properties of abelian varieties resp. Jacobians of curves. **Example**
Assume that there is a cover

$$\varphi : C \to \mathbb{P}^1;\ \deg \varphi = d,$$

in which one point (P_∞) is totally ramified and induces the place $(X = \infty)$ in the function field $\mathbb{F}_q(X)$ of $\mathbb{P}^1$.

Let O be the normal closure of $\mathbb{F}_q[X]$ in the function field of C.
Then ϕ is an isomorphism.

Examples for curves having such covers are all curves with a rational Weierstraß point, especially C_{ab}-curves and most prominently **hyperelliptic curves** including **elliptic curves**
as well as superelliptic curves.

Compared with the number theory case we have won a lot of freedom:
The parameters are:

1. p = characteristic of the base field

2. $n =$ degree of the ground field of $\mathbb{Z}/p$
3. $g_C = g =$ the genus of the curve C resp. the function field $Quot(O)$.

There are about $p^{3g\cdot n}$ curves of genus g over $\mathbb{F}_{p^n}$.

Structural relation: Hasse-Weil

$$\mid J_C(\mathbb{F}_{p^n} \mid \sim \; p^{ng}.$$

The **key length** is $n\,log(p) \cdot g$.

2 Hyperelliptic curves

Definition[2]
Assume that C is a projective irreducible non singular curve of genus ≥ 1 with a generically étale morphism ϕ of degree 2 to $\mathbb{P}^1$.
Then C is a **hyperelliptic curve**.
In terms of function fields this means:
The function field $F(C)$ of C is a separable extension of degree 2 of the rational function field $\mathbb{F}_q(X)$. Let ω denote the non trivial automorphism of this extension. It induces an involution ω on C with quotient $\mathbb{P}^1$.
The fixed points of ω are called
Weierstraß points.
Assume that we have a $\mathbb{F}_q$-rational Weierstraß point P_∞.
We choose ∞ on $\mathbb{P}^1$ as $\phi(P_\infty)$. Then the ring of holomorphic functions O on $C \setminus P_\infty$ is equal to the integral closure of $\mathbb{F}_q[X]$ in $F(C)$:

$$O = \mathbb{F}_q[X,Y]/f_C(X,Y)$$

where $f_C(X,Y)$ is a polynomial of degree 2 in Y and of degree $2g+1$ in X.

Theorem: $J_C(\mathbb{F}_q) = Pic(O)$.

[2] Elliptic curves ($g = 1$) are included.

From the algebraic point of view we are in a very similar situation as in the case of class groups of imaginary quadratic fields.
In fact: Artin has generalized Gauß 's theory of ideal classes of imaginary quadratic number fields to hyperelliptic function fields connecting ideal classes of O with reduced quadratic forms of discriminant $D(f)$ and the addition $\oplus$ with the composition of such forms. This is the basis for the **Cantor algorithm** which can be written down "formally" and then leads to addition **formulas** or can be implemented as **algorithm**. Explicit formulas by T. Lange

Addition, $\deg u_1 = \deg u_2 = 2$		
Input	$[u_1, v_1], [u_2, v_2], u_i = x^2 + u_{i1}x + u_{i0}, v_i = v_{i1}x + v_{i0}$	
Output	$[u', v'] = [u_1, v_1] + [u_2, v_2]$	
Step	Expression	Operations
1	compute resultant r of u_1, u_2: $z_1 = u_{11} - u_{21},\ z_2 = u_{20} - u_{10},\ z_3 = u_{11}z_1 + z_2$; $r = z_2 z_3 + z_1^2 u_{10}$;	1S, 3M
2	compute almost inverse of u_2 modulo u_1 ($inv = r/u_2 \bmod u_1$): $inv_1 = z_1,\ inv_0 = z_3$;	
3	compute $s' = rs \equiv (v_1 - v_2)inv \bmod u_1$: $w_0 = v_{10} - v_{20},\ w_1 = v_{11} - v_{21},\ w_2 = inv_0 w_0,\ w_3 = inv_1 w_1$; $s'_1 = (inv_0 + inv_1)(w_0 + w_1) - w_2 - w_3(1 + u_{11}),\ s'_0 = w_2 - u_{10}w_3$; if $s'_1 = 0$ see below	5M
4	compute $s'' = x + s_0/s_1 = x + s'_0/s'_1$ and s_1: $w_1 = (rs'_1)^{-1} (= 1/r^2 s_1),\ w_2 = rw_1 (= 1/s'_1),\ w_3 = {s'}_1^2 w_1 (= s_1)$; $w_4 = rw_2 (= 1/s_1),\ w_5 = w_4^2,\ s''_0 = s'_0 w_2$;	I, 2S, 5M
5	compute $l' = s'' u_2 = x^3 + l'_2 x^2 + l'_1 x + l'_0$: $l'_2 = u_{21} + s''_0,\ l'_1 = u_{21}s''_0 + u_{20},\ l'_0 = u_{20}s''_0$	2M
6	compute $u' = (s(l + h + 2v_2) - k)/u_1 = x^2 + u'_1 x + u'_0$: $u'_0 = (s''_0 - u_{11})(s''_0 - z_1 + h_2 w_4) - u_{10} + l'_1 + (h_1 + 2v_{21})w_4 + (2u_{21} + z_1 - f_4)w_5$; $u'_1 = 2s''_0 - z_1 + h_2 w_4 - w_5$;	3M
7	compute $v' \equiv -h - (l + v_2) \bmod u' = v'_1 x + v'_0$: $w_1 = l'_2 - u'_1,\ w_2 = u'_1 w_1 + u'_0 - l'_1,\ v'_1 = w_2 w_3 - v_{21} - h_1 + h_2 u'_1$; $w_2 = u'_0 w_1 - l'_0,\ v'_0 = w_2 w_3 - v_{20} - h_0 + h_2 u'_0$;	4M
total		I, 3S, 22M
Special case $s = s_0$		
$4'$	compute s: $inv = 1/r,\ s_0 = s'_0 inv$;	I, M
$5'$	compute $u' = (k - s(l + h + 2v_2))/u_1 = x + u'_0$: $u'_0 = f_4 - u_{21} - u_{11} - s_0^2 - s_0 h_2$;	S
$6'$	compute $v' \equiv -h - (l + v_2) \bmod u' = v'_0$: $w_1 = s_0(u_{21} + u'_0) + h_1 + v_{21} + h_2 u'_0,\ w_2 = s_0 + v_{20} + h_0$; $v'_0 = u'_0 w_1 - w_2$;	2M
total		I, 2S, 11M

Doubling, $\deg u = 2$			
Input	$[u, v], u = x^2 + u_1x + u_0, v = v_1x + v_0$		
Output	$[u', v'] = 2[u, v]$		

Step	Expression	odd	even
1	compute $\tilde{v} \equiv (h + 2v) \bmod u = \tilde{v}_1x + \tilde{v}_0$: $\tilde{v}_1 = h_1 + 2v_1 - h_2u_1,\ \tilde{v}_0 = h_0 + 2v_0 - h_2u_0$;		
2	compute resultant $r = \mathrm{res}(\tilde{v}, u)$: $w_0 = v_1^2,\ w_1 = u_1^2,\ w_2 = \tilde{v}_1^2,\ w_3 = u_1\tilde{v}_1,\ r = u_0w_2 + \tilde{v}_0(\tilde{v}_0 - w_3)$;;	2S, 3M $(w_2 = 4w_0)$	2S, 3M (see below)
3	compute almost inverse $inv' = invr$: $inv'_1 = -\tilde{v}_1,\ inv'_0 = \tilde{v}_0 - w_3$;		
4	compute $k' = (f - hv - v^2)/u \bmod u = k'_1x + k'_0$: $w_3 = f_3 + w_1,\ w_4 = 2u_0,\ k'_1 = 2(w_1 - f_4u_1) + w_3 - w_4 - v_1h_2$; $k'_0 = u_1(2w_4 - w_3 + f_4u_1 + v_1h_2) + f_2 - w_0 - 2f_4u_0 - v_1h_1 - v_0h_2$;	1M	2M (see below)
5	compute $s' = k'inv' \bmod u$: $w_0 = k'_0inv'_0,\ w_1 = k'_1inv'_1$; $s'_1 = (inv'_0 + inv'_1)(k'_0 + k'_1) - w_0 - w_1(1 + u_1),\ s'_0 = w_0 - u_0w_1$; If $s_1 = 0$ see below	5M	5M
6	compute $s'' = x + s_0/s_1$ and s_1: $w_1 = 1/(rs'_1)(= 1/r^2s_1),\ w_2 = rw_1(= 1/s'_1),\ w_3 = {s'}_1^2w_1(= s_1)$; $w_4 = rw_2(= 1/s_1),\ w_5 = w_4^2,\ s''_0 = s'_0w_2$;	I, 2S, 5M	I, 2S, 5M
7	compute $l' = s''u = x^3 + l'_2x^2 + l'_1x + l'_0$: $l'_2 = u_1 + s''_0,\ l'_1 = u_1s''_0 + u_0,\ l'_0 = u_0s''_0$;	2M	2M
8	compute $u' = s^2 + (h + 2v)s/u + (v^2 + hv - f)/u^2$: $u'_0 = {s''_0}^2 + w_4(h_2(s''_0 - u_1) + 2v_1 + h_1) + w_5(2u_1 - f_4)$; $u'_1 = 2s''_0 + w_4h_2 - w_5$;	S, 2M	S, M
9	compute $v' \equiv -h - (l + v) \bmod u' = v'_1x + v'_0$: $w_1 = l'_2 - u'_1,\ w_2 = u'_1w_1 + u'_0 - l'_1,\ v'_1 = w_2w_3 - v_1 - h_1 + h_2u'_1$; $w_2 = u'_0w_1 - l'_0,\ v'_0 = w_2w_3 - v_0 - h_0 + h_2u'_0$;	4M	4M
total		I, 5S, 22 M	I, 5S, 22 M

Special case $s = s_0$			
$6'$	compute s and precomputations: $w_1 = 1/r,\ s_0 = s'_0w_1,\ w_2 = u_0s_0 + v_0 + h_0$;	I,2M	I,2M
$7'$	compute $u' = (f - hv - v^2)/u^2 - (h + 2v)s/u - s^2$: $u'_0 = f_4 - s_0^2 - s_0h_2 - 2u_1$;	S	S
$8'$	compute $v' \equiv -h - (su + v) \bmod u'$: $w_1 = s_0(u_1 - u'_0) - h_2^2u'_0 + v_1 + h_1,\ v'_0 = u'_0w_1 - w_2$;	2M	2M
total		I, 3S, 13M	I, 3S, 14M

2.1 Non hyperelliptic curves of genus 3

Picard curves
or more generally
plane curves of genus 3
given by

$$Y^3 + f_1(X)Y = f(X)$$

with $deg(f) = 4$
have an efficient arithmetic too! (cf. e.g. work of Flon-Oyono).

2.2 Index-Calculus

As in the analogous situation in number theory there exists a subexponential attack based on the index-calculus principle.
But there is **one essential difference:** Recall: In the number field case the subexponential function was a function in $\mid D \mid$ and so of the order of the class group.
Due to Weil the analogue would be q^g.
But in the known index-calculus algorithm one cannot look at q and g as independent variables.
For instance: If $g = 1$ fixed then we do not get a subexponential attack for $q \to \infty$!. The attack:
The ideal classes of S can be represented by two polynomials of degrees bounded by g.
Choose as factor base for the index-calculus attack the ideal classes which can be represented by polynomials of small degrees.

Enge-Stein:
For $g/\log(q) > t$ the discrete logarithm in the divisor class group of a hyperelliptic curve of genus g defined over $\mathbb{F}_q$ can be computed with complexity bounded by $L_{1/2,q^g}[\frac{5}{\sqrt{6}}((1+\frac{3}{2t})^{1/2} + (\frac{3}{2t})^{1/2})]$.

This is for large genus a strong result.
Gaudry has a result much more serious for practical use: For hyperelliptic

curves of relatively small genus (in practice: $g \leq 9$) there is an index-calculus attack of complexity

$$O(q^2(\log(q))^\gamma)$$

with "reasonable small" constants.

Principle:
Use prime divisors of small degree (e.g. 1) as factor base.
A refinement is due to recent work of Theriault:
The complexity of the DL in hyperelliptic curves of genus g is bounded by

$$O(g^5 \cdot q^{2-\frac{4}{2g+1}+\epsilon})$$

. For $g = 4$ we get a bound $4^5 \cdot q^{1.56}$ (instead of q^2 generically).
For $g = 3$ we get $3^5 \cdot q^{1.43}$ instead of $q^{1.5}$.

"Result": Orders related to curves with rational Weierstraß points of genus ≥ 4 or closely related abelian varieties should be avoided!

State of the art: We have only three types of rings O which avoid serious index-calculus attacks and for which $Pic(O)$ in manageable:
MAXIMAL ORDERS BELONGING TO CURVES OF GENUS 1,2,3 (and even $g = 3$ is a little bit in danger)!