An attack on the elliptic curve discrete logarithm problem

Ayan Mahalanobis

IISER Pune

18 Feb 2023

Joint work with Vivek M. Mallick and Ansari Abdullah

Elliptic curve discrete logarithm problem

1. Elliptic curve discrete logarithm problem was first proposed by Miller (1985) and Koblitz (1987).

Elliptic curve discrete logarithm problem

1. Elliptic curve discrete logarithm problem was first proposed by Miller (1985) and Koblitz (1987).
2. Let $\mathcal{E}$ be the set of rational points of an elliptic curve, which is also a group under addition and a point at infinity. For sake of simplicity assume that $\mathcal{E}$ is of prime order p and P is its generator. Then ECDLP is: given P and $Q = mP$ find m.

Elliptic curve discrete logarithm problem

1. Elliptic curve discrete logarithm problem was first proposed by Miller (1985) and Koblitz (1987).
2. Let $\mathcal{E}$ be the set of rational points of an elliptic curve, which is also a group under addition and a point at infinity. For sake of simplicity assume that $\mathcal{E}$ is of prime order p and P is its generator. Then ECDLP is: given P and $Q = mP$ find m.
3. This primitive is used widely.

Elliptic curve discrete logarithm problem

1. Elliptic curve discrete logarithm problem was first proposed by Miller (1985) and Koblitz (1987).
2. Let $\mathcal{E}$ be the set of rational points of an elliptic curve, which is also a group under addition and a point at infinity. For sake of simplicity assume that $\mathcal{E}$ is of prime order p and P is its generator. Then ECDLP is: given P and $Q = mP$ find m.
3. This primitive is used widely.
4. This primitive is under constant attack.

Elliptic curve discrete logarithm problem

1. Elliptic curve discrete logarithm problem was first proposed by Miller (1985) and Koblitz (1987).
2. Let $\mathcal{E}$ be the set of rational points of an elliptic curve, which is also a group under addition and a point at infinity. For sake of simplicity assume that $\mathcal{E}$ is of prime order p and P is its generator. Then ECDLP is: given P and $Q = mP$ find m.
3. This primitive is used widely.
4. This primitive is under constant attack.
5. We present another attack. This attack is not generic and is Las Vegas in nature.

The main theorem

Theorem

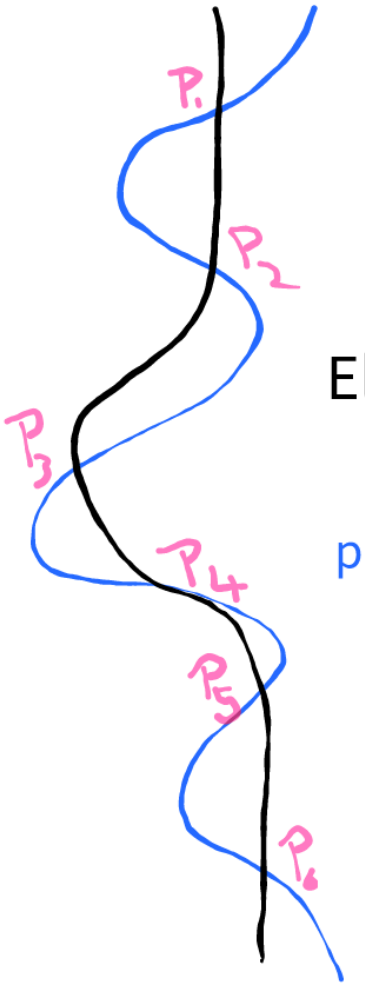
If a plane projective curve $\mathcal{C}$ of degree n' passes through the elliptic curve $\mathcal{E}$ at $3n'$ points $\{P_1, P_2, \ldots, P_{3n'}\}$ then $\sum_{i=1}^{3n'} P_i = \mathcal{O}$.

Proof.

Follows from the Abel-Jacobi's theorem that $P \mapsto [P] - [\mathcal{O}]$ is an isomorphism for an elliptic curve. □

Corollary

The above translates to if $P_i = n_i P$ where $0 < n_i < p$ above then $\sum_{i=1}^{3n'} n_i = 0 \mod p$. Note that $o(P) = p$ is a prime.



Elliptic curve

plane projective curve

1. Let $\mathcal{C} = \sum_{i+j+k=n'} x^i y^j z^k$ be an arbitrary plane projective curve of degree n'.
2. Compute $\mathcal{C}(P)$ as a row in a matrix $\mathcal{M}$. There is a fixed ordering in monomials.

$$\mathcal{M} = \begin{pmatrix} \mathcal{C}(P_1) \\ \mathcal{C}(P_2) \\ \vdots \\ \mathcal{C}(P_{3n'}) \end{pmatrix}$$

left kernel vs. right kernel

1. The right kernel of $\mathcal{M}$ contains all the curves $\mathcal{C}$ that passes through those points $\{P_i\}_{i=1}^{3n'}$.

left kernel vs. right kernel

1. The right kernel of $\mathcal{M}$ contains all the curves $\mathcal{C}$ that passes through those points $\{P_i\}_{i=1}^{3n'}$.
2. One idea is to compute the right kernel and find that curve.

left kernel vs. right kernel

1. The right kernel of $\mathcal{M}$ contains all the curves $\mathcal{C}$ that passes through those points $\{P_i\}_{i=1}^{3n'}$.
2. One idea is to compute the right kernel and find that curve.

Theorem

The left kernel $\mathcal{K}$ of $\mathcal{M}$ is non-zero if and only if there is a curve $\mathcal{C}$ passing through $3n'$ points of the elliptic curve.

Extra points (the real theorem)

Theorem

Let $k = 3n'$ for some positive integer n'. Let l be another positive integer. Choose positive integers s and t such that $s \neq t$ but $s + t = k + l$. Then construct the matrix $\mathcal{M}$ as described earlier. rows corresponding to $n_i P$ for $i = 1, 2, \ldots s$ and $-n_j Q$ for $j = 1, 2, \ldots, t$.
Let $\mathcal{K}$ be the left-kernel of $\mathcal{M}$. Then the following is true:

The left=kernel $\mathcal{K}$ is of dimension l.

If there is a vector v in $\mathcal{K}$ with l zeros then there is a curve $\mathcal{C}$ passing through $3n'$ points corresponding ot the non-zero points of v.

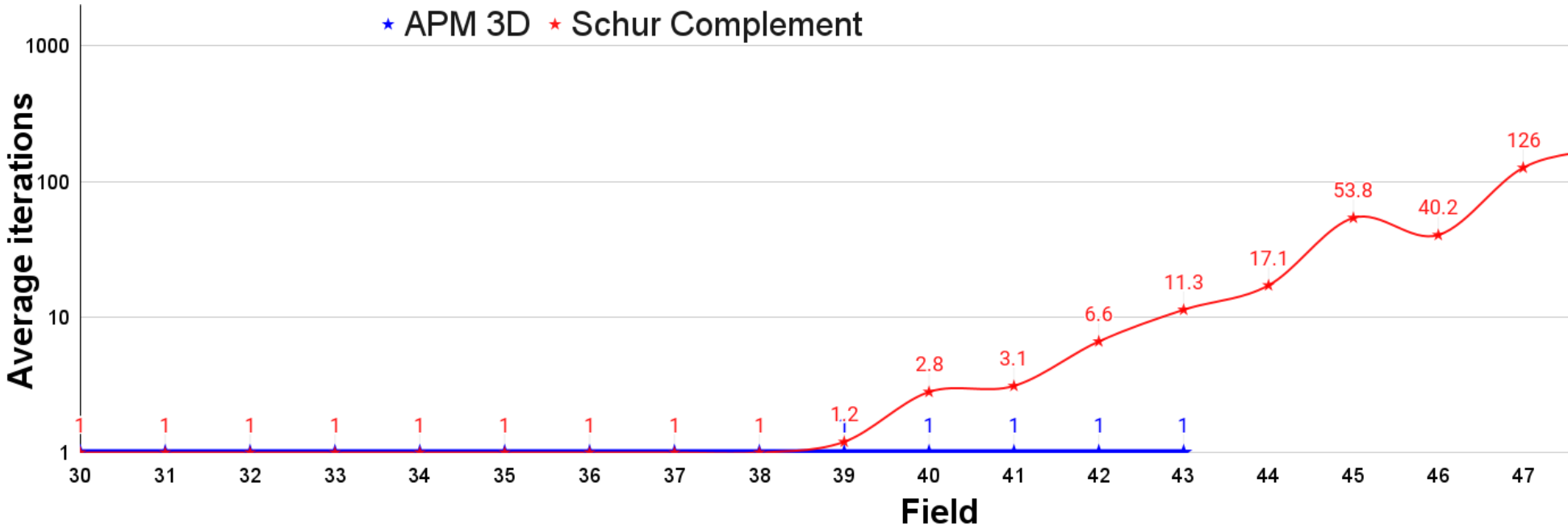
zero minors to solve ECDLP

$$\mathcal{K} = \begin{pmatrix} a_{11} & a_{12} & a_{13} & \dots & a_{1n} & 0 & 0 & \dots & 0 & 1 \\ a_{21} & a_{22} & a_{23} & \dots & a_{2n} & 0 & 0 & \dots & 1 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{n1} & a_{n2} & a_{n3} & \dots & a_{nn} & 1 & 0 & \dots & 0 & 0 \end{pmatrix}$$

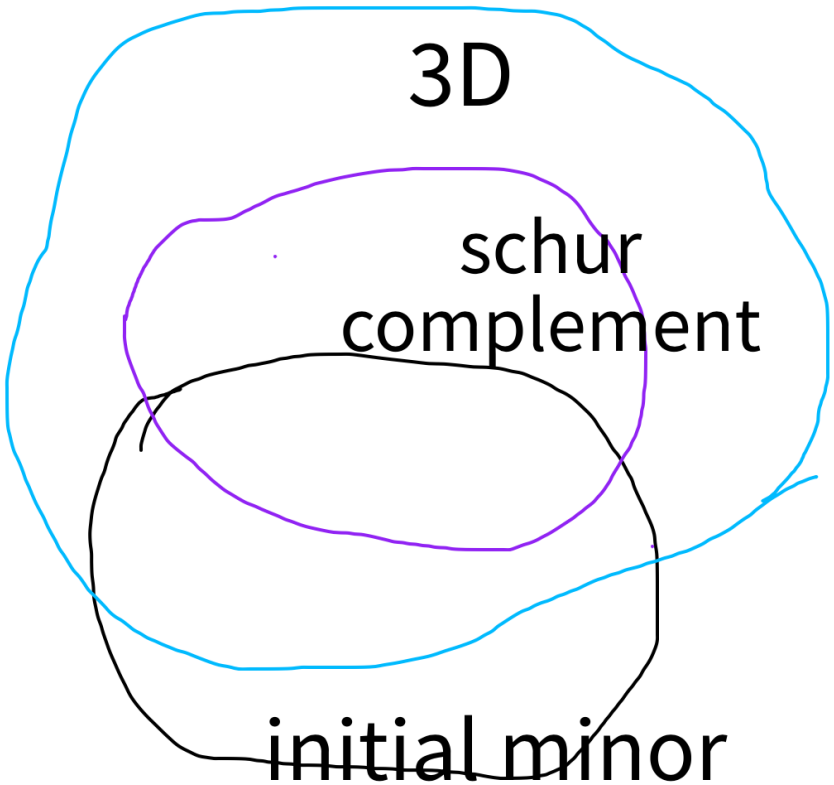
$$\mathcal{A} = \begin{pmatrix} a_{11} & a_{12} & a_{13} & \dots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \dots & a_{2n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & a_{n3} & \dots & a_{nn} \end{pmatrix}$$

Here $\mathcal{K}$ is a basis of the left kernel and the rows are the basis vectors of that subspace. Find a zero minor in $\mathcal{A}$.

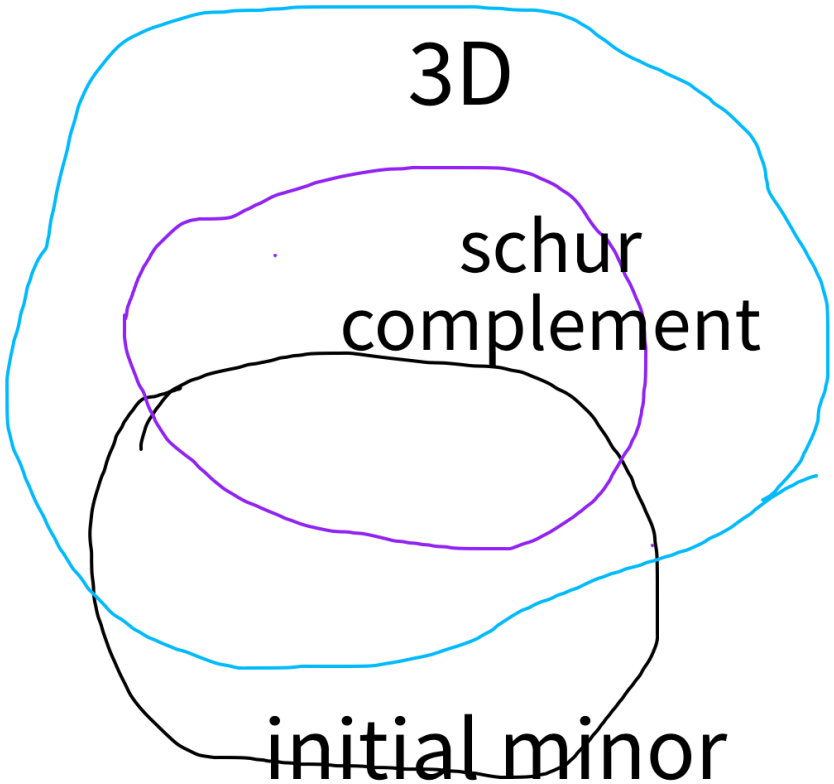
A graph – are we on the right track?



Last slide – what is going on?



Last slide – what is going on?



Conjecture (Initial minors)

For any matrix $\mathcal{M}$, there is a set of minors such if every minor in that set is non-zero then all minors are non-zero.