What is Index Calculus?

Claus Diem

University of Leipzig

Historical background

Let p be a prime number. Then a *primitive root* modulo p is a natural number $A < p$ such that for every natural number B coprime to p there exists some $e \in \mathbb{N}_0$ such that $A^e \equiv B \bmod p$.

Historical background

Let p be a prime number. Then a *primitive root* modulo p is a natural number $A < p$ such that for every natural number B coprime to p there exists some $e \in \mathbb{N}_0$ such that $A^e \equiv B \bmod p$.

Fact I. Primitive roots modulo prime numbers always exist.

Fact II. "Little Fermat" $A^{p-1} \equiv 1 \bmod p$.

Historical background

Let p be a prime number. Then a *primitive root* modulo p is a natural number $A < p$ such that for every natural number B coprime to p there exists some $e \in \mathbb{N}_0$ such that $A^e \equiv B \bmod p$.

Fact I. Primitive roots modulo prime numbers always exist.

Fact II. "Little Fermat" $A^{p-1} \equiv 1 \bmod p$.

Gauß defines in the "Disquisitiones Arithmeticae" (1801): Let A be a primitive root modulo p, and let B an integer coprime to p. Then the *index* of B modulo p to the base A is the residue class of numbers $e \in \mathbb{N}_0$ with $A^e \equiv B \bmod p$.

Historical background

This definition immediately generates to natural numbers n which have a primitive root A.

Historical background

This definition immediately generates to natural numbers n which have a primitive root A.

Fact III. A primitive root modulo n exists if and only if n is 1,2,4, p^k or $2p^k$ for an odd prime p and $k \in \mathbb{N}$.

Historical background

This definition immediately generates to natural numbers n which have a primitive root A.

Fact III. A primitive root modulo n exists if and only if n is 1,2,4, p^k or $2p^k$ for an odd prime p and $k \in \mathbb{N}$.

We set $\mathrm{ind}_A(B) := e$ if e is the smallest natural number with $A^e \equiv B \bmod n$.

Historical background

This definition immediately generates to natural numbers n which have a primitive root A.

Fact III. A primitive root modulo n exists if and only if n is 1,2,4, p^k or $2p^k$ for an odd prime p and $k \in \mathbb{N}$.

We set $\mathrm{ind}_A(B) := e$ if e is the smallest natural number with $A^e \equiv B \bmod n$.

Indices should be viewed as ”discrete analogs” of logarithms.

If $n = p$ is a prime number then
$\mathrm{ind}_A(B \cdot C) \equiv \mathrm{ind}_A(B) + \mathrm{ind}_A(C) \bmod p - 1$.

Historical background

Obvious task. Compute tables of indices, analogously to tables of logarithms.

In 1839 Jacobi published a book of all indices modulo any prime power ≤ 1000.

Historical background

Obvious task. Compute tables of indices, analogously to tables of logarithms.

In 1839 Jacobi published a book of all indices modulo any prime power ≤ 1000.

Question. How can one efficiently compute the index of just one number or the indices of the number below a certain bound?

Maurice Kraitchik gave a method in his book ”Théorie des Nombres” (1922). The method is based on collecting relations and linear algebra. It was called the *index calculus method* by Odklyzko in 1985.

Historical background

A cryptographic application Alice and Bob want to establish a common key for an encrypted session "in public".

Alice and Bob agree on a prime p and a primitive root A

Alice		Bob
Chooses $x \in \{1, \ldots p-1\}$		Chooses $y \in \{1, \ldots p-1\}$
	$\xrightarrow{X := A^x \bmod p}$	
	$\xleftarrow[Y := A^y \bmod p]{}$	

Now $X^y \equiv A^{xy} \equiv Y^x \bmod p$.

The (original) index calculus method

Idea. Let p be a prime, and let A be a primitive root modulo p. Let us fix a number S, and let $P_1, \ldots, P_k$ be the prime numbers $\leq S$.
Now one searches for *relations* of the form

$$\prod_j P_j^{r_j} \equiv A^r \bmod p\ .$$

The (original) index calculus method

Idea. Let p be a prime, and let A be a primitive root modulo p. Let us fix a number S, and let $P_1, \ldots, P_k$ be the prime numbers $\leq S$.

Now one searches for *relations* of the form

$$\prod_j P_j^{r_j} \equiv A^r \bmod p \ .$$

Such a relation can be rewritten as

$$\prod_j A^{\mathrm{ind}_A(P_j) r_j} \equiv A^r \bmod p \ ,$$

The (original) index calculus method

Idea. Let p be a prime, and let A be a primitive root modulo p. Let us fix a number S, and let $P_1, \ldots, P_k$ be the prime numbers $\leq S$.

Now one searches for *relations* of the form

$$\prod_j P_j^{r_j} \equiv A^r \bmod p \,.$$

Such a relation can be rewritten as

$$\prod_j A^{\mathrm{ind}_A(P_j) r_j} \equiv A^r \bmod p \,,$$

and this leads to a linear relation on indices:

$$\sum_j r_j \,\mathrm{ind}_A(P_j) \equiv r \bmod p-1$$

An example

Let $p = 83, A = 2, S = 7$ such that $P_1 = 2, P_2 = 3, P_3 = 5, P_4 = 7$.

An example

Let $p = 83, A = 2, S = 7$ such that $P_1 = 2, P_2 = 3, P_3 = 5, P_4 = 7$.

We have (modulo $p = 83$):

$$2^1 \equiv \quad 2$$

An example

Let $p = 83, A = 2, S = 7$ such that $P_1 = 2, P_2 = 3, P_3 = 5, P_4 = 7$.

We have (modulo $p = 83$):

$$2^1 \equiv 2$$
$$2^7 \equiv 45 = 3^2 \cdot 5$$

An example

Let $p = 83, A = 2, S = 7$ such that $P_1 = 2, P_2 = 3, P_3 = 5, P_4 = 7$.

We have (modulo $p = 83$):

$$\begin{aligned} 2^1 &\equiv 2 \\ 2^7 &\equiv 45 = 3^2 \cdot 5 \\ 2^8 &\equiv 7 \end{aligned}$$

An example

Let $p = 83, A = 2, S = 7$ such that
$P_1 = 2, P_2 = 3, P_3 = 5, P_4 = 7$.

We have (modulo $p = 83$):

$$\begin{aligned}
2^1 &\equiv \quad 2 \\
2^7 &\equiv \quad 45 = 3^2 \cdot 5 \\
2^8 &\equiv \quad 7 \\
2^9 &\equiv \quad 14 = 2 \cdot 7
\end{aligned}$$

An example

Let $p = 83, A = 2, S = 7$ such that
$P_1 = 2, P_2 = 3, P_3 = 5, P_4 = 7$.

We have (modulo $p = 83$):

$$
\begin{aligned}
2^1 &\equiv 2 \\
2^7 &\equiv 45 = 3^2 \cdot 5 \\
2^8 &\equiv 7 \\
2^9 &\equiv 14 = 2 \cdot 7 \\
2^{10} &\equiv 28 = 2^2 \cdot 7
\end{aligned}
$$

An example

Let $p = 83, A = 2, S = 7$ such that
$P_1 = 2, P_2 = 3, P_3 = 5, P_4 = 7$.

We have (modulo $p = 83$):

$$
\begin{aligned}
2^1 &\equiv 2 \\
2^7 &\equiv 45 = 3^2 \cdot 5 \\
2^8 &\equiv 7 \\
2^9 &\equiv 14 = 2 \cdot 7 \\
2^{10} &\equiv 28 = 2^2 \cdot 7 \\
2^{11} &\equiv 56 = 2^3 \cdot 7
\end{aligned}
$$

An example

Let $p = 83, A = 2, S = 7$ such that $P_1 = 2, P_2 = 3, P_3 = 5, P_4 = 7$.

We have (modulo $p = 83$):

$$
\begin{aligned}
2^1 &\equiv 2 \\
2^7 &\equiv 45 = 3^2 \cdot 5 \\
2^8 &\equiv 7 \\
2^9 &\equiv 14 = 2 \cdot 7 \\
2^{10} &\equiv 28 = 2^2 \cdot 7 \\
2^{11} &\equiv 56 = 2^3 \cdot 7 \\
2^{12} &\equiv 29
\end{aligned}
$$

An example

Let $p = 83, A = 2, S = 7$ such that
$P_1 = 2, P_2 = 3, P_3 = 5, P_4 = 7$.

We have (modulo $p = 83$):

$$
\begin{aligned}
2^1 &\equiv 2 \\
2^7 &\equiv 45 = 3^2 \cdot 5 \\
2^8 &\equiv 7 \\
2^9 &\equiv 14 = 2 \cdot 7 \\
2^{10} &\equiv 28 = 2^2 \cdot 7 \\
2^{11} &\equiv 56 = 2^3 \cdot 7 \\
2^{12} &\equiv 29 \\
2^{13} &\equiv 58 = 2 \cdot 29
\end{aligned}
$$

An example

Let $p = 83, A = 2, S = 7$ such that $P_1 = 2, P_2 = 3, P_3 = 5, P_4 = 7$.

We have (modulo $p = 83$):

$$
\begin{aligned}
2^1 &\equiv 2 \\
2^7 &\equiv 45 = 3^2 \cdot 5 \\
2^8 &\equiv 7 \\
2^9 &\equiv 14 = 2 \cdot 7 \\
2^{10} &\equiv 28 = 2^2 \cdot 7 \\
2^{11} &\equiv 56 = 2^3 \cdot 7 \\
2^{12} &\equiv 29 \\
2^{13} &\equiv 58 = 2 \cdot 29 \\
2^{14} &\equiv 33 = 2 \cdot 11
\end{aligned}
$$

An example

Let $p = 83, A = 2, S = 7$ such that $P_1 = 2, P_2 = 3, P_3 = 5, P_4 = 7$.

We have (modulo $p = 83$):

$$
\begin{aligned}
2^1 &\equiv 2 \\
2^7 &\equiv 45 = 3^2 \cdot 5 \\
2^8 &\equiv 7 \\
2^9 &\equiv 14 = 2 \cdot 7 \\
2^{10} &\equiv 28 = 2^2 \cdot 7 \\
2^{11} &\equiv 56 = 2^3 \cdot 7 \\
2^{12} &\equiv 29 \\
2^{13} &\equiv 58 = 2 \cdot 29 \\
2^{14} &\equiv 33 = 2 \cdot 11 \\
2^{15} &\equiv 66 = 2^2 \cdot 11
\end{aligned}
$$

An example

Let $p = 83, A = 2, S = 7$ such that $P_1 = 2, P_2 = 3, P_3 = 5, P_4 = 7$.

We have (modulo $p = 83$):

$$
\begin{aligned}
2^1 &\equiv 2 \\
2^7 &\equiv 45 = 3^2 \cdot 5 \\
2^8 &\equiv 7 \\
2^9 &\equiv 14 = 2 \cdot 7 \\
2^{10} &\equiv 28 = 2^2 \cdot 7 \\
2^{11} &\equiv 56 = 2^3 \cdot 7 \\
2^{12} &\equiv 29 \\
2^{13} &\equiv 58 = 2 \cdot 29 \\
2^{14} &\equiv 33 = 2 \cdot 11 \\
2^{15} &\equiv 66 = 2^2 \cdot 11 \\
2^{16} &\equiv 49 = 7^2
\end{aligned}
$$

An example

Let $p = 83, A = 2, S = 7$ such that $P_1 = 2, P_2 = 3, P_3 = 5, P_4 = 7$.

We have (modulo $p = 83$):

$$
\begin{aligned}
2^1 &\equiv 2 \\
2^7 &\equiv 45 = 3^2 \cdot 5 \\
2^8 &\equiv 7 \\
2^9 &\equiv 14 = 2 \cdot 7 \\
2^{10} &\equiv 28 = 2^2 \cdot 7 \\
2^{11} &\equiv 56 = 2^3 \cdot 7 \\
2^{12} &\equiv 29 \\
2^{13} &\equiv 58 = 2 \cdot 29 \\
2^{14} &\equiv 33 = 2 \cdot 11 \\
2^{15} &\equiv 66 = 2^2 \cdot 11 \\
2^{16} &\equiv 49 = 7^2 \\
2^{17} &\equiv 15 = 3 \cdot 5
\end{aligned}
$$

An example (cont.)

This gives the following linear system over $\mathbb{Z}/82\mathbb{Z}$:

2	3	5	7		
1	0	0	0	1	
0	2	1	0	7	
0	0	0	1	8	
(1	0	0	1	9)	
0	1	1	0	17	
0	1	0	0	-10	= 72
0	0	1	0	34 - 7	= 27

An example (cont.)

This gives the following linear system over $\mathbb{Z}/82\mathbb{Z}$:

2	3	5	7		
1	0	0	0	1	
0	2	1	0	7	
0	0	0	1	8	
(1	0	0	1	9)	
0	1	1	0	17	
0	1	0	0	-10	= 72
0	0	1	0	34 - 7	= 27

Thus $\mathrm{ind}_2(2) = 1, \mathrm{ind}_2(3) = 72, \mathrm{ind}_2(5) = 27, \mathrm{ind}_2(7) = 8$.

An example (cont.)

This gives the following linear system over $\mathbb{Z}/82\mathbb{Z}$:

2	3	5	7		
1	0	0	0	1	
0	2	1	0	7	
0	0	0	1	8	
(1	0	0	1	9)	
0	1	1	0	17	
0	1	0	0	-10	= 72
0	0	1	0	34 - 7	= 27

Thus $\mathrm{ind}_2(2) = 1, \mathrm{ind}_2(3) = 72, \mathrm{ind}_2(5) = 27, \mathrm{ind}_2(7) = 8$.

What is $\mathrm{ind}_2(31)$?

An example (cont.)

This gives the following linear system over $\mathbb{Z}/82\mathbb{Z}$:

2	3	5	7		
1	0	0	0	1	
0	2	1	0	7	
0	0	0	1	8	
(1	0	0	1	9)	
0	1	1	0	17	
0	1	0	0	-10	= 72
0	0	1	0	34 - 7	= 27

Thus $\text{ind}_2(2) = 1, \text{ind}_2(3) = 72, \text{ind}_2(5) = 27, \text{ind}_2(7) = 8$.

What is $\text{ind}_2(31)$? We have $31^2 \equiv 48 = 2^4 \cdot 3$, thus $2 \cdot \text{ind}_2(31) \equiv 4 + 72 = 76$, and therefore $\text{ind}_2(31) = 38$ or $\text{ind}_2(31) \equiv 38 + 41 = 79$. In fact, $\text{ind}_2(31) = 38$.

Result

Theorem. Given a prime number p, a primitive root A modulo p and some $B < p$, one can compute the index of B modulo p with respect to A in an expected time of

$$\exp\left((\sqrt{2}+o(1))\cdot(\log(p)\cdot\log\log(p))^{1/2}\right) .$$

Result

Theorem. Given a prime number p, a primitive root A modulo p and some $B < p$, one can compute the index of B modulo p with respect to A in an expected time of

$$\exp\left((\sqrt{2}+o(1)) \cdot (\log(p) \cdot \log\log(p))^{1/2}\right) .$$

This is *subexponential* in $\log(p)$.

A generalization

Definition. Let $(G, \cdot)$ be any finite group, and let $a, b \in G$ with $b \in \langle a \rangle$. Then the *discrete logarithm* of b with respect to a is the smallest non-negative integer e with $a^e = b$.

If G, a, b are explicitly given, an obvious task is to compute the discrete logarithm.

A generalization

Definition. Let $(G, \cdot)$ be any finite group, and let $a, b \in G$ with $b \in \langle a \rangle$. Then the *discrete logarithm* of b with respect to a is the smallest non-negative integer e with $a^e = b$.

If G, a, b are explicitly given, an obvious task is to compute the discrete logarithm.

Up to now we studied the case of $G = \mathbb{F}_p^*$ and $a = [A]_p$ a generator of G.

An obvious generalization is $G = \mathbb{F}_q^*$. (Again $\mathbb{F}_q^*$ is cyclic.)

A generalization

How fast can one compute discrete logarithms in arbitrary groups?

A generalization

How fast can one compute discrete logarithms in arbitrary groups?

Theorem. Given G, a, b and $\mathrm{ord}(a)$, one can compute the discrete logarithm of b with respect to a with $\mathcal{O}(\sqrt{\mathrm{ord}(a)})$ group operations.

A generalization

How fast can one compute discrete logarithms in arbitrary groups?

Theorem. Given G, a, b and $\operatorname{ord}(a)$, one can compute the discrete logarithm of b with respect to a with $\mathcal{O}(\sqrt{\operatorname{ord}(a)})$ group operations.

Idea. Consider multiples a^k and b^ℓ until one has found some k, ℓ with $a^k = b^\ell$. If then ℓ is invertible modulo $\operatorname{ord}(a)$, we have $e = \frac{k}{\ell} \in \mathbb{Z}/\operatorname{ord}(a)\mathbb{Z}$.

One has to perform fewer tries than one expects naïvely (*birthday paradox*).

A generalization

How fast can one compute discrete logarithms in arbitrary groups?

Theorem. Given G, a, b and $\operatorname{ord}(a)$, one can compute the discrete logarithm of b with respect to a with $\mathcal{O}(\sqrt{\operatorname{ord}(a)})$ group operations.

Idea. Consider multiples a^k and b^ℓ until one has found some k, ℓ with $a^k = b^\ell$. If then ℓ is invertible modulo $\operatorname{ord}(a)$, we have $e = \frac{k}{\ell} \in \mathbb{Z}/\operatorname{ord}(a)\mathbb{Z}$.

One has to perform fewer tries than one expects naïvely (*birthday paradox*).

If $\operatorname{ord}(a)$ is not prime, one can also reduce to computations ”modulo the prime factors” (Chinese Remainer Theorem).

On the possibility of index calculus

An index calculus algorithm proceeds in these steps:

- Fix a suitable subset $\mathcal{G} := \{p_1, \ldots, p_k\} \subseteq G$
- Collect relations between the input elements and the p_i.
- Compute the discrete logarithm via linear algebra.

On the possibility of index calculus

We now write the group law *additively*. This means: Given $a, b \in G$ with $b \in \langle a \rangle$, the discrete logarithm of b with respect to a is the smallest non-negative integer e with $e \cdot a = b$.

A general index calculus algorithm

We do not assume anymore that a is a generting element of G. But we assume that $\mathrm{ord}(a)$ is known.

Let us assume that we have some procedure which under input of G, a suitable subset $\{p_1, \ldots, p_k\} \subseteq G$ and an element $g \in G$ outputs with a certain probability a relation $\sum_j r_j p_j = g$. Then we have the following ”general algorithm”:

On the possibility of index calculus

A general index calculus algorithm

- Fix a suitable subset $\mathcal{G} := \{p_1, \dots, p_k\} \subseteq G$.
- Find $k+1$ relations $\sum_j r_{i,j} p_j = \alpha_i a + \beta_i b$, let $R = ((r_{i,j}))_{i,j}$, $\underline{\alpha} := (\alpha_i)_i, \underline{\beta} := (\beta_i)_i$.
- Compute some non-trivial vector $\underline{\gamma} \in (\mathbb{Z}/\operatorname{ord}(a)\mathbb{Z})^{1\times(k+1)}$ with $\underline{\gamma} R = 0$.
- We now have $\sum_i \gamma_i \alpha_i a + \sum_i \gamma_i \beta_i b = 0$. Thus if $\sum_i \gamma_i \beta_i \in (\mathbb{Z}/\operatorname{ord}(a)\mathbb{Z})^*$, then $e := -(\sum_i \gamma_i \alpha_i)(\sum_i \gamma_i \beta_i)^{-1}$ is the discrete logarithm of b with respect to a.

On the ”classical” index calculus

Back to the ”classical case”: Let p be a prime number. We consider discrete logarithms in $\mathbb{F}_p^*$. Let $\mathbb{N}' := \{n \in \mathbb{N} \mid p \nmid n\}$. Note that $(\mathbb{N}', \cdot)$ is a free abelian monoid on $\mathcal{P} - \{p\}$.

We have a surjective homomorphism of monoids

$$\mathbb{N}' \longrightarrow \mathbb{F}_p^*,\ N \mapsto [N]_p \ .$$

Moreover we have a canonical ”lifting” (a section) $\mathbb{F}_p^* \longrightarrow \mathbb{N}'$ given by $[N]_p \mapsto N$ if $1 \leq N < p$.

On the ”classical” index calculus

Back to the ”classical case”: Let p be a prime number. We consider discrete logarithms in $\mathbb{F}_p^*$. Let $\mathbb{N}' := \{n \in \mathbb{N} \mid p \nmid n\}$. Note that $(\mathbb{N}', \cdot)$ is a free abelian monoid on $\mathcal{P} - \{p\}$.

We have a surjective homomorphism of monoids

$$\mathbb{N}' \longrightarrow \mathbb{F}_p^*,\ N \mapsto [N]_p \ .$$

Moreover we have a canonical ”lifting” (a section) $\mathbb{F}_p^* \longrightarrow \mathbb{N}'$ given by $[N]_p \mapsto N$ if $1 \leq N < p$.

In fact, the surjection $\mathbb{N}' \longrightarrow \mathbb{F}_p^*$ induces a surjection of groups $(\mathbb{Z}_{(p)})^* \longrightarrow \mathbb{F}_p^*$, and $(\mathbb{Z}_{(p)})^* \simeq \{\pm 1\} \times \mathbb{Z}^{(\mathcal{P}-\{p\})}$.

On the ”classical” index calculus

As above, let $S > 0$ Let $P_1, \ldots, P_k$ be the prime number $\leq S$, and let $p_i := [P_i]_p$.

Now let $n \in \mathbb{F}_p^*$. Then we proceed as follows:

- ”Lift” n to $\mathbb{N}$, that is, let N be the unique representative $< p$ of n.
- Try to factorize N over $\{P_1, \ldots, P_k\}$.
- If N factorizes as $N = \prod_j P_j^{r_j}$, then we have the relation $n = \prod_j p_j^{r_j}$.

Finite fields of of small characteristic

Let now $q = p^n$ with p ”small”.

Let $\mathbb{F}_q = \mathbb{F}_p[X]/(f)$. Then we have a surjection

$$(\mathbb{F}_p[X]_{(f)})^* \longrightarrow \mathbb{F}_q^*$$

Again we can ”lift elements” and proceed similarly.

A challange

Task. Find (families of) groups for which the fastest known algorithms to compute discrete logarithms are the ”generic algorithms”!

A challange

Task. Find (families of) groups for which the fastest known algorithms to compute discrete logarithms are the ”generic algorithms”!

Finite fields are ruled out.

A challange

Task. Find (families of) groups for which the fastest known algorithms to compute discrete logarithms are the ”generic algorithms”!

Finite fields are ruled out.

In 1987 Miller and Koblitz (independently) suggested the groups of rational points of elliptic curves over finite fields.

Elliptic curves

Definition (one possibility). An elliptic curve over a field K is a cubic in $\mathbb{P}^2_K$ together with a fixed K-rational point.

General definition. Let V be any variety over a field K. Then $V(K)$ is the set of points in V with coordinates in K.

Elliptic curves

Definition (one possibility). An elliptic curve over a field K is a cubic in $\mathbb{P}^2_K$ together with a fixed K-rational point.

General definition. Let V be any variety over a field K. Then $V(K)$ is the set of points in V with coordinates in K.

Fact. Let $E/K : F(X, Y, Y) = 0$ with $O \in E(K)$ be an elliptic curve. Then $E(K)$ is ”in an obvious way” an abelian group.

The rule is: Three points on one line add up to O. (The group law is written *additively*.)

Elliptic curves

Definition (one possibility). An elliptic curve over a field K is a cubic in $\mathbb{P}^2_K$ together with a fixed K-rational point.

General definition. Let V be any variety over a field K. Then $V(K)$ is the set of points in V with coordinates in K.

Fact. Let $E/K : F(X,Y,Y) = 0$ with $O \in E(K)$ be an elliptic curve. Then $E(K)$ is "in an obvious way" an abelian group.

The rule is: Three points on one line add up to O. (The group law is written *additively*.)

Fact. For elliptic curves over finite fields, we have $\#E(\mathbb{F}_q) \sim q$ for $q \longrightarrow \infty$.

On the possibility of index calculus

Is some kind of ”lifting” possible for elliptic curves?

On the possibility of index calculus

Is some kind of ”lifting” possible for elliptic curves?

Let $\mathcal{E}$ be an ”elliptic curve” over $\mathbb{Z}_{(p)}$ which ”reduces to” $E/\mathbb{F}_p$. Let E_η be the corresponding elliptic curve over $\mathbb{Q}$. We again have a map

$$\mathcal{E}(\mathbb{Z}_{(p)}) \longrightarrow E(\mathbb{F}_p),$$

and $\mathcal{E}(\mathbb{Z}_{(p)})$ is included in $E_\eta(\mathbb{Q})$.

On the possibility of index calculus

Is some kind of ”lifting” possible for elliptic curves?

Let $\mathcal{E}$ be an ”elliptic curve” over $\mathbb{Z}_{(p)}$ which ”reduces to” $E/\mathbb{F}_p$. Let E_η be the corresponding elliptic curve over $\mathbb{Q}$. We again have a map

$$\mathcal{E}(\mathbb{Z}_{(p)}) \longrightarrow E(\mathbb{F}_p),$$

and $\mathcal{E}(\mathbb{Z}_{(p)})$ is included in $E_\eta(\mathbb{Q})$.

However, $E_\eta(\mathbb{Q})$ is always finitely generated (Theorem of Mordell-Weil).

On the possibility of index calculus

Another approach:

Let q be any prime number, and let E be any elliptic curve over $\mathbb{F}_q$. Then we have the isomorphism

$$E(K) \longrightarrow \mathrm{Cl}^0(E)\ , P \mapsto [P] - [O]\ .$$

On the possibility of index calculus

Another approach:

Let q be any prime number, and let E be any elliptic curve over $\mathbb{F}_q$. Then we have the isomorphism

$$E(K) \longrightarrow \mathrm{Cl}^0(E)\ , P \mapsto [P] - [O]\ .$$

Let C/K be any smooth projective curve. Then we have a surjection $\mathrm{Div}^0(C) \longrightarrow \mathrm{Cl}^0(C/K)$, and again $\mathrm{Div}^0(C/K)$ is a free abelian group. Moreover, we have a ”more or less canonical” lifting.

On the possibility of index calculus

Another approach:

Let q be any prime number, and let E be any elliptic curve over $\mathbb{F}_q$. Then we have the isomorphism

$$E(K) \longrightarrow \mathrm{Cl}^0(E)\ , P \mapsto [P] - [O]\ .$$

Let C/K be any smooth projective curve. Then we have a surjection $\mathrm{Div}^0(C) \longrightarrow \mathrm{Cl}^0(C/K)$, and again $\mathrm{Div}^0(C/K)$ is a free abelian group. Moreover, we have a ”more or less canonical” lifting.

This can be used for index calculus. However:

On the possibility of index calculus

Another approach:

Let q be any prime number, and let E be any elliptic curve over $\mathbb{F}_q$. Then we have the isomorphism

$$E(K) \longrightarrow \mathrm{Cl}^0(E)\ , P \mapsto [P] - [O]\ .$$

Let C/K be any smooth projective curve. Then we have a surjection $\mathrm{Div}^0(C) \longrightarrow \mathrm{Cl}^0(C/K)$, and again $\mathrm{Div}^0(C/K)$ is a free abelian group. Moreover, we have a ”more or less canonical” lifting.

This can be used for index calculus. However:

For an elliptic curve the lifting is given by $P \longleftrightarrow [P] - [O] \mapsto (P) - (O)$. This is ”too easy”. (No factorization possible.)

On the possibility of index calculus

There is an ”algebraic approach” for elliptic curves over *extension fields* which works (Gaudry, D.):

Let $q = p^n$ for a prime number p. Let E be an elliptic curve over $\mathbb{F}_q$, given by $y^2 = f(x)$.

Now let

$$\mathcal{G} := \{P \in E(\mathbb{F}_p) \mid x(P) \in \mathbb{F}_p\} \; .$$

Then one can generate relations by solving multivariate systems over $\mathbb{F}_p$.

A result

One can obtain:

Theorem (D.) Let $\epsilon > 0$. Then one can solve the discrete logarithm problem in elliptic curves over finite fields of the form $\mathbb{F}_{p^n}$ with $(2+\epsilon) \cdot n^2 \leq \log_2(p)$ in an expected time which is polynomial in p.

A result

Corollary Let again $\epsilon > 0$, and let $a > 2 + \epsilon$. Then one can solve the discrete logarithm problem in elliptic curves over finite fields of the form $\mathbb{F}_{p^n}$ with $(2+\epsilon) \cdot n^2 \leq \log_2(p) \leq a \cdot n^2$ in an expected time of

$$e^{\mathcal{O}(1) \cdot (\log(p^n))^{2/3}} .$$

A result

Corollary Let again $\epsilon > 0$, and let $a > 2 + \epsilon$. Then one can solve the discrete logarithm problem in elliptic curves over finite fields of the form $\mathbb{F}_{p^n}$ with $(2+\epsilon)\cdot n^2 \leq \log_2(p) \leq a \cdot n^2$ in an expected time of

$$e^{\mathcal{O}(1)\cdot(\log(p^n))^{2/3}} \; .$$

Indeed, the expected running time is polynomial in

$$p = 2^{\log_2(p)} = 2^{(\log_2(p))^{(1+1/2)\cdot 2/3}} \leq 2^{(\sqrt{a}\cdot n \log_2(p))^{2/3}} \; .$$