Berechnung diskreter Logarithmen und Faktorisierung

Claus Diem

Im Sommersemester 2019

Berechnung diskreter Logarithmen

Einteilung

- Generische Verfahren

Einteilung

- Generische Verfahren
- Relationensuch- und Lineare Algebra-Verfahren

Einteilung

- Generische Verfahren

  “Benutze nur, dass Du eine Gruppe hast!”

- Relationensuch- und Lineare Algebra-Verfahren

Einteilung

- Generische Verfahren

  “Benutze nur, dass Du eine Gruppe hast!”

- Relationensuch- und Lineare Algebra-Verfahren

  oder Logarithmentafel-Verfahren

Generische Verfahren

Setting

Wir betrachten ein DLP:

Z.B. in

- $\mathbf{F}_p^*$, p prim
- $\mathbf{F}_q^*$, q Primpotenz
- $\mathbf{F}_{p^e}^*$, p feste Primzahl (oder Primpotenz), $e \in \mathbf{N}$
- ....

Sei $(G; a, b)$ eine Instanz:

G ist eine endliche Gruppe,

$a, b \in G$, $b \in \langle a \rangle$.

1. Chinesischer Restsatz

Voraussetzung.

Es ist eine Faktorisierung von $\operatorname{ord}(a)$ oder von $\#G$ bekannt

1. Chinesischer Restsatz

Voraussetzung.

Es ist eine Faktorisierung von $\operatorname{ord}(a)$ oder von $\#G$ bekannt / gegeben

1. Chinesischer Restsatz

Voraussetzung.

Es ist eine Faktorisierung von $\mathrm{ord}(a)$ oder von $\#G$ bekannt / gegeben , oder allgemeiner:

$$\mathrm{ord}(a) \mid \ell_1 \cdot \ell_2 \quad \text{mit} \quad \ell_1, \ell_2 \neq 1 \text{ teilerfremd}$$

1. Chinesischer Restsatz

Voraussetzung.

Es ist eine Faktorisierung von $\mathrm{ord}(a)$ oder von $\#G$ bekannt / gegeben , oder allgemeiner:

$$\mathrm{ord}(a) \mid \ell_1 \cdot \ell_2 \quad \text{mit} \quad \ell_1, \ell_2 \neq 1 \text{ teilerfremd}$$

Vorgehen.

- Löse die Instanzen $(G; a^{\ell_2}, b^{\ell_2}), (G; a^{\ell_1}, b^{\ell_1})$,
- setze die Lösungen mit den Chinesichen Restsatz zusammen.

Reduktion

1. Chinesischer Restsatz

Voraussetzung.

Es ist eine Faktorisierung von $\mathrm{ord}(a)$ oder von $\#G$ bekannt / gegeben , oder allgemeiner:

$$\mathrm{ord}(a) \mid \ell_1 \cdot \ell_2 \quad \text{mit} \quad \ell_1, \ell_2 \neq 1 \text{ teilerfremd}$$

Vorgehen.

- Löse die Instanzen $(G; a^{\ell_2}, b^{\ell_2}), (G; a^{\ell_1}, b^{\ell_1})$,
- setze die Lösungen mit den Chinesichen Restsatz zusammen.

2. Iterativ für $\#ord(a)$ eine Primpotenz

Die Baby-Step-Giant-Step-Methode

Sei weiterhin eine Instanz $(G; a, b)$ gegeben.

Vorausetzung. Es sei eine obere Schranke N an $\mathrm{ord}(a)$ bekannt / gegeben.

Idee. Sei $x \in \mathbf{N}_0$, $x \leq N$ "mögliche Lösung".

Sei $\ell := \lfloor \sqrt{N} + 1 \rfloor$.

Betrachte ℓ-adische Entwicklung: $x = x_0 + \ell x_1$:

$$a^x = b \longleftrightarrow a^{x_0 + \ell x_1} = b \longleftrightarrow a^{x_0} b^{-1} = a^{-\ell x_1}$$

Die Baby-Step-Giant-Step-Methode

$$a^x = b \longleftrightarrow a^{x_0+\ell x_1} = b \longleftrightarrow a^{x_0} b^{-1} = a^{-\ell x_1}$$

Algorithmus.

1. Setze $\ell \longleftarrow \lfloor \sqrt{N} + 1 \rfloor$.
2. Berechne Tupel $(0, x_0, a^{x_0} b^{-1})$, $(1, x_1, a^{-\ell x_1})$ für $x_0, x_1 = 0, \ldots, \ell$.
3. Sortiere die Tupel nach dem letzten Eintrag.
4. Gehe die Liste durch bis zu aufeinanderfolgenden Einträgen $(0, x_0, c)$, $(1, x_1, c)$ für ein c.
5. Gib $x \longleftarrow x_0 + \ell x_1$ aus.

Die Schranke N kann auch kleiner als $\mathrm{ord}(a)$ sein. Dann funktioniert's vielleicht nicht.

Die Baby-Step-Giant-Step-Methode

$$a^x = b \longleftrightarrow a^{x_0+\ell x_1} = b \longleftrightarrow a^{x_0} b^{-1} = a^{-\ell x_1}$$

Algorithmus.

1. Setze $\ell \longleftarrow \lfloor \sqrt{N} + 1 \rfloor$.
2. Berechne Tupel $(0, x_0, a^{x_0} b^{-1})$, $(1, x_1, a^{-\ell x_1})$ für $x_0, x_1 = 0, \ldots, \ell$.
3. Sortiere die Tupel nach dem letzten Eintrag.
4. Gehe die Liste durch bis zu aufeinanderfolgenden Einträgen $(0, x_0, c)$, $(1, x_1, c)$ für ein c.
5. Gib $x \longleftarrow x_0 + \ell x_1$ aus.

Die Schranke N kann auch kleiner als $\mathrm{ord}(a)$ sein. Dann funktioniert's vielleicht nicht.

Wir können N auch schritweise erhöhen, z.B. $N = 2^k$.

Die Baby-Step-Giant-Step-Methode

Satz. Das diskrete Logarithmusproblem in $\mathbf{F}_q^*$ kann in einer Zeit von

$$O(\sqrt{\mathrm{ord}(a)} \cdot \log(\mathrm{ord}(a)) \cdot \log(q)^2)$$

mit einer TM gelöst werden.

Die Rho-Methode

Charakteristika.

Die Rho-Methode

Charakteristika.

- Variante mit minimalem Speicherplatz.

Die Rho-Methode

Charakteristika.

- Variante mit minimalem Speicherplatz.
- Die Laufzeitanalyse ist heuristisch.

Die Rho-Methode

Charakteristika.

- Variante mit minimalem Speicherplatz.
- Die Laufzeitanalyse ist heuristisch.
- Es muss ein Vielfaches der Gruppenordnung bekannt sein.

Die Rho-Methode

Beschreibung (einer Variante)

Sei $(G; a, b)$ eine Instanz.

Unterteile die Gruppe G in drei Teile (pseudozufällig):

$$G = X_1 \dot\cup X_2 \dot\cup X_3$$

Betrachte "nächstes-Element-Funktion"

$$f : G \longrightarrow G \ , \ g \mapsto \begin{cases} ag & \text{für } g \in X_1 \\ g^2 & \text{für } g \in X_2 \\ bg & \text{für } g \in X_3 \end{cases}$$

Die Rho-Methode

Beschreibung (einer Variante)

Sei $(G; a, b)$ eine Instanz.

Unterteile die Gruppe G in drei Teile (pseudozufällig):

$$G = X_1 \dot\cup X_2 \dot\cup X_3$$

Betrachte "nächstes-Element-Funktion"

$$f : G \longrightarrow G \ , \ g \mapsto \begin{cases} ag & \text{für } g \in X_1 \\ g^2 & \text{für } g \in X_2 \\ bg & \text{für } g \in X_3 \end{cases}$$

und damit:

$$g_0 = 1_G$$
$$g_{i+1} = f(g_i)$$

Die Rho-Methode

$$g_0 = 1_G$$
$$g_{i+1} = f(g_i)$$

Die g_i haben die Form $a^{\alpha_i} b^{\beta_i}$.

Wenn eine Kollision $g_j = g_{j+k}$ gegeben ist:

$$a^{\alpha_j} b^{\beta_j} = a^{\alpha_{j+k}} b^{\beta_{j+k}}$$

$$a^{\alpha_j - \alpha_{j+k}} = b^{-(\beta_j - \beta_{j+k})}$$

Für ein Vielfaches N von $\mathrm{ord}(a)$ und $[\alpha_j - \alpha_{j+k}]_N$ invertierbar:

$$b = a^{-\frac{[\alpha_j - \alpha_{j+k}]_N}{[\beta_i - \beta_{j+k}]_N}}$$

Fragen

1. Wie findet man eine Kollision?
2. Wie lange dauert das?

Kollisionssuche und danach

1. Speichere für ein betrachtetes Element g_i auch die Zusammensetzung $a^{\alpha_i} b^{\beta_i}$ ab.

Kollisionssuche und danach

1. Speichere für ein betrachtetes Element g_i auch die Zusammensetzung $a^{\alpha_i} b^{\beta_i}$ ab.
2. Wenn $g_j = g_{j+k}$, dann auch $g_{j'} = g_{j'+k}$ für alle $j' \geq j$.

   Eine Möglichkeit:

Kollisionssuche und danach

1. Speichere für ein betrachtetes Element g_i auch die Zusammensetzung $a^{\alpha_i} b^{\beta_i}$ ab.
2. Wenn $g_j = g_{j+k}$, dann auch $g_{j'} = g_{j'+k}$ für alle $j' \geq j$.

   Eine Möglichkeit:
   Für $i = (i_\ell \dots i_0)_2$:

Kollisionssuche und danach

1. Speichere für ein betrachtetes Element g_i auch die Zusammensetzung $a^{\alpha_i} b^{\beta_i}$ ab.
2. Wenn $g_j = g_{j+k}$, dann auch $g_{j'} = g_{j'+k}$ für alle $j' \geq j$.

   Eine Möglichkeit:
   Für $i = (i_\ell \dots i_0)_2$:
   Vergleiche stets g_i mit $g_{(i_\ell 0 \dots 0)_2}$.

Kollisionssuche und danach

1. Speichere für ein betrachtetes Element g_i auch die Zusammensetzung $a^{\alpha_i} b^{\beta_i}$ ab.
2. Wenn $g_j = g_{j+k}$, dann auch $g_{j'} = g_{j'+k}$ für alle $j' \geq j$.

   Eine Möglichkeit:
   Für $i = (i_\ell \dots i_0)_2$:
   Vergleiche stets g_i mit $g_{(i_\ell 0 \dots 0)_2}$.

   - Es müssen stets nur zwei Gruppenelemente betrachtet werden (und abgespeichert sein) (+ Zerlegungen der Elemente).

Kollisionssuche und danach

1. Speichere für ein betrachtetes Element g_i auch die Zusammensetzung $a^{\alpha_i} b^{\beta_i}$ ab.
2. Wenn $g_j = g_{j+k}$, dann auch $g_{j'} = g_{j'+k}$ für alle $j' \geq j$.

   Eine Möglichkeit:
   Für $i = (i_\ell \dots i_0)_2$:
   Vergleiche stets g_i mit $g_{(i_\ell 0 \dots 0)_2}$.

   - Es müssen stets nur zwei Gruppenelemente betrachtet werden (und abgespeichert sein) (+ Zerlegungen der Elemente).
   - Laufzeit höchstens "Faktor 2" vom Optimum entfernt.

Die Rho-Methode

Laufzeit

Wie lange dauert es so bis zu einer Kollision?

Geburtstagsparadox: Schneller, als man denkt ...

Die Rho-Methode

Laufzeit

Wie lange dauert es so bis zu einer Kollision?

Geburtstagsparadox: Schneller, als man denkt ...

Unter heuristischen Annahmen:

Die Rho-Methode

Laufzeit

Wie lange dauert es so bis zu einer Kollision?

Geburtstagsparadox: Schneller, als man denkt ...

Unter heuristischen Annahmen:

Man braucht etwa $\sqrt{\text{ord}(a)}$ Iterationen.

Die Relationen und Lineare Algebra-Methode

Die Relationen und Lineare Algebra-Methode

oder

Die Logarithmentafel-Methode

Die Relationen und Lineare Algebra-Methode

oder

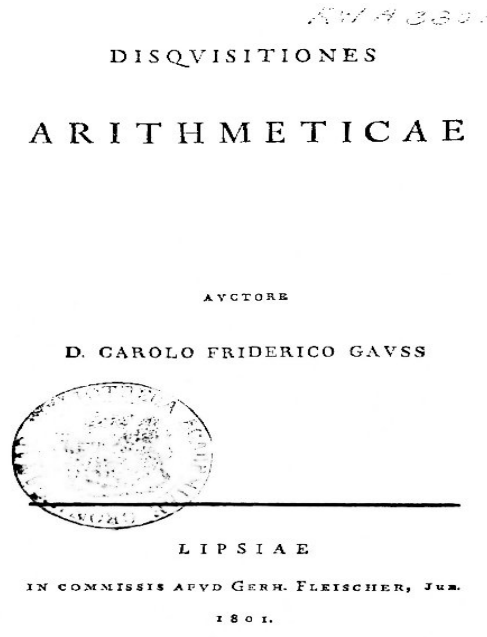
Die Logarithmentafel-Methode

oder

Die Indexkalkül-Methode

Gauß und die Disquisitiones Arithmeticae

* 1777



DISQVISITIONES

ARITHMETICAE

AVCTORE

D. CAROLO FRIDERICO GAVSS

LIPSIAE

IN COMMISSIS APVD GERH. FLEISCHER, Jun.

1801

1801

1906. 2015.

Carl Friedrich Gauss'

Untersuchungen über höhere Arithmetik.

(Disquisitiones arithmeticae. Theorematis arithmetici demonstratio nova. Summatio quarumdam serierum singularium. Theorematis fundamentalis in doctrina de residuis quadraticis demonstrationes et ampliationes novae. Theoria residuorum biquadraticorum, commentatio prima et secunda. Etc.)

Deutsch herausgegeben

von

H. Maser.

Berlin.
Verlag von Julius Springer.
1889.

Hieraus folgt, dass der Exponent, zu welchem A gehört, ein Teiler von $\frac{p-1}{a}$ (Artikel 48) d. i. $\frac{p-1}{a^{\alpha+1}}$ eine ganze Zahl sein muss. Nun kann aber $\frac{p-1}{a^{\alpha+1}} = \frac{b^\beta c^\gamma \dots}{a}$ keine ganze Zahl sein (Artikel 15); somit müssen wir endlich schliessen, dass unsere Annahme nicht richtig sein kann, dass vielmehr das Product $ABC \dots$ wirklich zum Exponenten $p-1$ gehört.

Der letztere Beweis scheint etwas weitläufiger als der erste, dieser aber dafür weniger direct zu sein als jener.

56.

Dieser Satz liefert ein ausgezeichnetes Beispiel dafür, wie grosse Vorsicht oft in der Theorie der Zahlen erforderlich ist, damit man nicht das für ausgemacht annehme, was es in Wirklichkeit nicht ist, Lambert erwähnt in seiner schon oben angeführten Abhandlung, *Acta Erudit. 1769 p. 127,* diesen Satz, ohne auch nur von der Notwendigkeit eines Beweises zu reden. Niemand aber hat den Beweis versucht ausser Euler: *Comment. nov. Ac. Petrop. T. XVIII für das Jahr 1773, Demonstrationes circa residua ex divisione potestatum per numeros primos resultantia p. 85 u. ff.* Man sehe besonders Artikel 37, wo er sich über die Notwendigkeit eines Beweises weitläufiger auslässt. Doch leidet der Beweis, welchen der scharfsinnige Autor giebt, an zwei Mängeln. Der eine besteht darin, dass er im Artikel 31 u. ff. stillschweigend annimmt, dass die Congruenz $x^n \equiv 1$ (mit Übertragung der dort angewandten Redeweise in unsere Bezeichnung) wirklich n verschiedene Wurzeln habe, obwohl vorher nur bewiesen worden ist, dass sie nicht mehr als n Wurzeln haben kann; der andere ist der, dass er die Formel des Artikels 34 nur durch Induction abgeleitet hat.

Primitive Wurzeln, Grundzahlen, Indices.

57.

Die zum Exponenten $p-1$ gehörigen Zahlen werden wir mit Euler **primitive Wurzeln** nennen. Wenn also a eine primitive Wurzel ist, so werden die kleinsten Reste der Potenzen $a, a^2, a^3, \dots, a^{p-1}$ sämtlich von einander verschieden sein, woraus sich leicht ergiebt, dass sich unter diesen alle Zahlen $1, 2, 3, \dots, p-1$, deren Anzahl ebenso gross ist, wie die jener kleinsten Reste, vorfinden müssen, d. h. dass jede durch p nicht teilbare Zahl irgend einer Potenz von a congruent ist. Diese ausgezeichnete Eigenschaft ist von dem grössten Nutzen und kann die arithmetischen, auf die Congruenzen bezüglichen Operationen sehr erheblich erleichtern, etwa in derselben Weise, wie die Einführung der Logarithmen die Operationen der gemeinen Arithmetik. Wir werden nach Belieben irgend eine

primitive Wurzel a als **Basis** oder **Grundzahl** annehmen und auf diese alle durch p nicht teilbaren Zahlen beziehen, und wenn $a^e \equiv b \pmod{p}$ ist, so werden wir e den **Index** von b nennen. Wenn z. B. für den Modul 19 die primitive Wurzel 2 als Basis genommen wird, so werden

den Zahlen	1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	13.	14.	15.	16.	17.	18.
die Indices	0.	1.	13.	2.	16.	14.	6.	3.	8.	17.	12.	15.	5.	7.	11.	4.	10.	9

entsprechen. Übrigens ist klar, dass, wenn die Basis dieselbe bleibt, einer jeden Zahl mehrere Indices zukommen, dass aber diese sämtlich nach dem Modul $p-1$ congruent sind. So oft daher von den Indices die Rede sein wird, werden diejenigen, welche nach dem Modul $p-1$ congruent sind, als äquivalent betrachtet werden, ähnlich wie die Zahlen selbst, wenn sie nach dem Modul p congruent sind, als äquivalent gelten.

Algorithmus der Indices.

58.

Die auf die Indices bezüglichen Sätze sind durchaus analog denen, welche für die Logarithmen gelten.

Der Index des Products aus beliebig vielen Factoren ist der Summe der Indices der einzelnen Factoren nach dem Modul $p-1$ congruent.

Der Index der Potenz irgend einer Zahl ist dem Producte aus dem Index der gegebenen Zahl und dem Exponenten der Potenz nach dem Modul $p-1$ congruent.

Die Beweise lassen wir ihrer Leichtigkeit halber weg.

Hieraus ist ersichtlich, dass, wenn man eine Tafel construieren wollte, aus der man die Indices aller Zahlen für verschiedene Moduln entnehmen könnte, aus derselben sowohl alle Zahlen, welche grösser als der Modul sind, als auch alle zusammengesetzten Zahlen fortgelassen werden könnten. Eine Probe einer solchen Tafel ist am Schlusse dieses Werkes als Tafel I angefügt. Auf derselben stehen in der ersten Vertikalreihe die Primzahlen und deren Potenzen von 3 bis 97, die als Moduln zu betrachten sind, neben jeder von ihnen die zur Basis genommenen Zahlen; dann folgen die Indices der aufeinanderfolgenden Primzahlen, von denen immer je fünf durch einen kleinen Zwischenraum getrennt sind; in derselben Weise sind am Kopfe der Tafel die Primzahlen angeordnet, so dass man leicht und sicher finden kann, welcher Index einer gegebenen Primzahl nach einem gegebenen Modul entspricht.

Ist z. B. $p = 67$, so ist der Index der Zahl 60, wenn man 12 zur Basis nimmt:

$$\equiv 2 \text{ ind. } 2 + \text{ind. } 3 + \text{ind. } 5 \pmod{66} \equiv 58 + 9 + 39 \equiv 40.$$

59.

Der Index jedes Wertes des Ausdrucks $\frac{a}{b}$ (mod. p) (Artikel 31) ist nach dem Modul $p-1$ der Differenz der Indices des Zählers a und des Nenners b congruent, wofern die Zahlen a und b durch p nicht teilbar sind.

Ist nämlich c irgend ein Wert des Ausdrucks, so ist $bc \equiv a$ (mod. p), daher:

$$\text{ind. } b + \text{ind. } c \equiv \text{ind. } a \text{ (mod. } p-1)$$

und somit

$$\text{ind. } c \equiv \text{ind. } a - \text{ind. } b.$$

Wenn man daher eine Tafel hat, aus welcher der einer jeden Zahl nach jedem beliebigen Primzahlmodul entsprechende Index, und eine andere, aus welcher die zu einem gegebenen Index gehörige Zahl entnommen werden kann, so lassen sich sämtliche Congruenzen ersten Grades mit der grössten Leichtigkeit lösen, da man alle auf solche zurückführen kann, deren Modul eine Primzahl ist (Artikel 30). Ist z. B. die Congruenz $29x + 7 \equiv 0$ (mod. 47) vorgelegt, so wird: $x \equiv \frac{-7}{29}$ (mod. 47), also:

$$\text{ind. } x \equiv \text{ind. } (-7) - \text{ind. } 29 \equiv \text{ind. } 40 - \text{ind. } 29 \equiv 15 - 43 \equiv 18 \text{ (mod. } 46).$$

Der Index 18 aber gehört zur Zahl 3. Demnach ist $x \equiv 3$ (mod. 47).

Eine zweite Tafel haben wir allerdings nicht hinzugefügt, doch kann an Stelle dieser eine andere dienen, wie wir im sechsten Abschnitt zeigen werden.

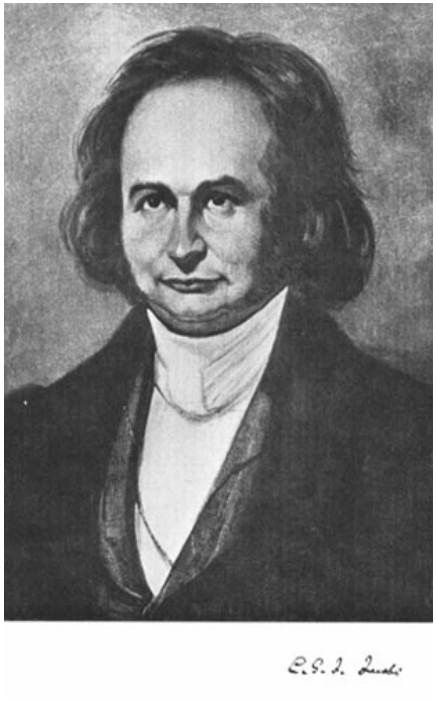
Über die Wurzeln der Congruenz $x^n \equiv A$.

60.

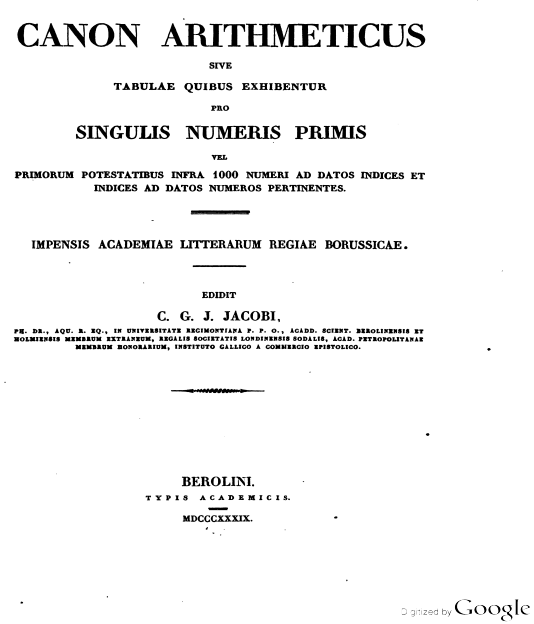
In analoger Weise, wie wir im Artikel 31 die Wurzeln der Congruenzen ersten Grades bezeichnet haben, werden wir im Folgenden auch die Wurzeln der reinen Congruenzen höherer Grade durch ein Zeichen darstellen. Wie nämlich $\sqrt[n]{A}$ nichts anderes bedeutet als eine Wurzel der Gleichung $x^n = A$, so wird mit Hinzufügung des Moduls durch $\sqrt[n]{A}$ (mod. p) jede beliebige Wurzel der Congruenz $x^n \equiv A$ (mod. p) bezeichnet werden. Wir werden sagen, dass dieser Ausdruck $\sqrt[n]{A}$ (mod. p) so viele Werte besitze, als er nach dem Modul p incongruente Werte hat, da sämtliche nach p congruente Werte als äquivalent zu betrachten sind (Artikel 26). Überdies ist klar, dass, wenn A und B nach dem Modul p congruent waren, die Ausdrücke $\sqrt[n]{A}$ (mod. p) und $\sqrt[n]{B}$ (mod. p) einander äquivalent sein werden.

Setzt man nun $\sqrt[n]{A} \equiv x$ (mod. p), so wird n ind. $x \equiv$ ind. A (mod. $p-1$). Aus dieser Congruenz ergeben sich nach den Regeln des vorigen

Tafeln von Indices = diskreten Logarithmen



C.G.J. Jacobi (*1804)



CANON ARITHMETICUS

SIVE

TABULAE QUIBUS EXHIBENTUR

PRO

SINGULIS NUMERIS PRIMIS

VEL

PRIMORUM POTESTATIBUS INFRA 1000 NUMERI AD DATOS INDICES ET INDICES AD DATOS NUMEROS PERTINENTES.

IMPENSIS ACADEMIAE LITTERARUM REGIAE BORUSSICAE.

EDIDIT

C. G. J. JACOBI,

PH. DR., AQU. R. EQ., IN UNIVERSITATE REGIOMONTANA P. P. O., ACADD. SCIENT. BEROLINENSIS ET HOLMIENSIS MEMBRUM EXTRANEUM, REGALIS SOCIETATIS LONDINENSIS SODALIS, ACAD. PETROPOLITANAE MEMBRUM HONORARIUM, INSTITUTO GALLICO A COMMERCIO EPISTOLICO.

BEROLINI.

TYPIS ACADEMICIS.

MDCCCXXXIX.

1849

$p = 499$

Numeri. $p-1 = 2 \cdot 3 \cdot 83$ **Indices.**

I	0	1	2	3	4	5	6	7	8	9
		10	100	2	20	200	4	40	400	8
1	80	301	16	160	103	32	320	206	64	141
2	412	128	282	325	256	65	151	13	130	302
3	26	260	105	52	21	210	104	42	420	208
4	84	341	416	168	183	333	336	366	167	173
5	233	334	346	466	169	193	433	338	386	367
6	177	273	235	354	47	470	209	94	441	418
7	188	383	337	376	267	175	253	35	350	7
8	70	201	14	140	402	28	280	305	56	61
9	111	112	122	222	224	244	444	448	488	389
10	397	477	279	295	455	59	91	411	118	182
11	323	236	364	147	472	229	294	445	458	89
12	391	417	178	283	335	356	67	171	213	134
13	342	426	268	185	353	37	370	207	74	241
14	414	148	482	329	296	465	159	93	431	318
15	186	363	137	372	227	274	245	454	49	490
16	409	98	481	319	196	463	139	392	427	278
17	285	355	57	71	211	114	142	422	228	284
18	345	456	69	191	413	138	382	327	276	265
19	155	53	31	310	106	62	121	212	124	242
20	424	248	484	349	496	469	199	493	439	398
21	487	379	297	475	259	95	451	19	190	403
22	38	380	307	76	261	115	152	23	230	304
23	46	460	109	92	421	218	184	343	436	368
24	187	373	237	374	247	474	249	494	449	498
25	489	399	497	479	299	495	459	99	491	419
26	198	483	339	396	467	179	293	435	358	87
27	371	217	174	243	434	348	486	369	197	473
28	239	394	447	478	289	395	457	79	291	415
29	158	83	331	316	166	163	133	332	326	266
30	165	153	33	330	306	66	161	113	132	322
31	226	264	145	452	29	290	405	58	81	311
32	116	162	123	232	324	246	464	149	492	429
33	298	485	359	97	471	219	194	443	438	388
34	387	377	277	275	255	55	51	11	110	102
35	22	220	204	44	440	408	88	381	317	176
36	263	135	352	27	270	205	54	41	410	108
37	82	321	216	164	143	432	328	286	365	157
38	73	231	314	146	462	129	292	425	258	85
39	351	17	170	203	34	340	406	68	181	313

N	0	1	2	3	4	5	6	7	8	9
		498	3	453	6	496	456	79	9	408
1	1	347	459	27	82	451	12	391	411	217
2	4	34	350	227	462	494	30	363	85	314
3	454	192	15	302	394	77	414	135	220	480
4	7	367	37	430	353	406	230	64	465	158
5	497	346	33	191	366	345	88	172	317	105
6	457	89	195	487	18	25	305	126	397	182
7	80	173	417	380	138	449	223	426	483	287
8	10	318	370	291	40	389	433	269	356	119
9	409	106	233	147	67	215	468	333	161	257
10	2	458	349	14	36	32	194	416	369	232
11	348	90	91	307	175	225	320	435	108	470
12	460	196	92	322	198	492	490	402	21	385
13	28	488	308	296	129	361	400	152	185	166
14	83	19	176	374	420	312	383	113	141	327
15	452	26	226	301	429	190	486	379	290	146
16	13	306	321	295	373	300	294	48	43	54
17	392	127	436	49	272	75	359	60	122	265
18	412	398	109	44	236	133	150	240	70	442
19	218	183	471	55	336	478	164	278	260	206
20	5	81	461	393	352	365	17	137	39	66
21	35	174	197	128	419	428	372	271	235	335
22	351	418	93	437	94	404	310	154	178	115
23	228	381	323	50	438	62	111	242	473	280
24	463	139	199	273	95	156	325	244	201	246
25	495	450	493	76	405	344	24	448	388	214
26	31	224	491	360	311	189	299	74	132	477
27	364	427	403	61	155	343	188	342	169	102
28	86	484	22	123	179	170	377	446	423	284
29	315	288	386	266	116	103	144	212	330	254
30	455	11	29	413	229	87	304	222	432	467
31	193	319	489	399	382	185	293	358	149	163
32	16	371	309	110	324	23	298	187	376	143
33	303	292	297	45	51	124	46	72	57	262
34	395	41	130	237	439	180	52	475	275	203
35	78	390	362	134	63	171	125	425	268	332
36	415	434	401	151	112	378	47	59	239	277
37	136	270	153	241	243	447	73	341	445	211
38	221	357	186	71	474	424	58	340	339	99
39	481	120	167	443	281	285	263	100	209	251

$p = 521$

Numeri. $p - 1 = 2^3 \cdot 5 \cdot 13$ **Indices.**

I	0	1	2	3	4	5	6	7	8	9
		439	472	371	317	56	97	382	457	38
1	10	222	31	63	44	39	449	173	402	380
2	100	136	310	109	440	390	322	167	373	153
3	479	318	495	48	232	253	94	107	83	488
4	101	54	261	480	236	446	419	28	309	191
5	489	19	5	111	276	292	22	280	485	347
6	201	190	50	68	155	315	220	195	161	344
7	447	337	500	159	508	24	116	387	47	314
8	302	244	311	27	391	240	118	223	470	14
9	415	356	505	270	263	316	138	146	11	140
10	503	434	361	95	25	34	338	418	110	358
11	341	172	484	429	250	340	254	12	58	454
12	284	157	151	122	416	274	456	120	59	372
13	235	7	468	178	513	135	392	158	69	73
14	266	70	512	217	441	308	273	17	169	209
15	55	179	431	86	242	475	125	170	127	6
16	29	227	142	339	336	61	208	137	228	60
17	290	186	378	264	234	89	517	328	196	79
18	295	297	133	35	256	369	481	154	397	269
19	345	365	288	350	476	43	121	498	323	85
20	324	3	275	374	71	430	168	291	104	329
21	114	30	145	93	189	132	117	305	519	164
22	98	300	408	409	327	278	128	445	501	77
23	459	395	433	443	144	175	238	282	321	249
24	422	303	162	262	398	187	296	215	84	406
25	52	425	57	15	333	307	355	66	319	413
26	520	82	49	150	204	465	424	139	64	483
27	511	299	490	458	477	482	72	348	119	141
28	421	385	211	412	81	131	199	354	148	368
29	42	203	26	473	289	268	427	414	438	33
30	420	467	260	41	285	75	102	493	212	330
31	32	502	516	410	245	229	499	241	36	174
32	320	331	471	453	366	206	301	326	360	177
33	74	184	21	362	13	497	405	134	474	207
34	219	277	210	494	130	281	403	298	51	507
35	106	165	16	251	258	205	383	375	510	381
36	18	87	160	426	496	487	183	103	411	163
37	180	349	37	92	271	181	267	509	463	67
38	237	364	370	399	105	247	65	401	462	149
39	286	514	53	343	8	386	129	363	452	448

N	0	1	2	3	4	5	6	7	8	9
		520	478	201	436	52	159	131	394	402
1	10	98	117	334	89	253	352	147	360	51
2	488	332	56	457	75	104	292	83	47	160
3	211	12	310	299	105	183	318	372	9	15
4	446	303	290	195	14	454	415	78	33	262
5	62	348	250	392	41	158	5	252	118	128
6	169	165	490	13	268	386	257	379	63	138
7	141	204	276	139	330	305	487	229	493	179
8	404	284	261	38	248	199	153	361	492	175
9	412	465	373	213	36	103	511	6	220	500
10	20	40	306	367	208	384	350	37	519	23
11	108	53	483	482	210	509	76	216	86	278
12	127	196	123	504	448	156	491	158	226	396
13	344	285	215	182	337	135	21	167	96	267
14	99	279	162	432	234	212	97	463	288	389
15	263	122	445	29	187	64	451	121	137	73
16	362	68	242	369	219	351	516	27	206	148
17	157	453	111	17	319	235	450	329	133	151
18	370	375	423	366	331	424	171	245	514	214
19	61	49	469	437	484	67	178	460	458	286
20	498	60	518	291	264	355	325	339	166	149
21	342	282	308	405	515	247	477	143	501	340
22	66	481	11	87	441	506	440	161	168	315
23	467	430	34	452	174	130	44	380	236	497
24	85	317	154	485	81	314	462	385	406	239
25	114	353	449	35	116	400	184	433	354	503
26	302	42	243	94	173	444	140	376	295	189
27	93	374	499	146	125	202	54	341	225	414
28	57	345	237	496	120	304	390	434	192	294
29	170	207	55	428	421	180	246	181	347	271
30	221	326	80	241	403	217	507	255	145	48
31	22	82	409	426	79	65	95	4	31	258
32	320	238	26	198	200	438	327	224	177	209
33	309	321	474	254	505	431	164	71	106	163
34	115	110	411	393	69	190	495	59	277	371
35	193	417	408	466	287	256	91	479	109	502
36	328	102	333	397	381	191	324	447	289	185
37	382	3	129	28	203	357	472	494	172	422
38	19	359	7	356	427	281	395	77	442	475
39	25	84	136	486	418	231	416	188	244	383

Tafeln von Indices

Sei eine Primzahl p gegeben.

Notation.

Ganze Zahlen: $A, B, \ldots$

Restklassen modulo p: $a, b, \ldots$.

Es sei A eine Primitivwurzel, d.h. $a := [A]_p$ ist ein Erzeugendes von $\mathbf{F}_p$.

Wir interessieren uns für die diskreten Logarithmen zur Basis a

oder anders:

für die Indices modulo p zur Primitivwurzel A.

Tafeln von Indices

Ziel. Wir wollen eine partielle Tafel benutzen und trotzdem (ziemlich) effizient Indices / diskrete Logarithmen berechnen.

Tafeln von Indices

Ziel. Wir wollen eine partielle Tafel benutzen und trotzdem (ziemlich) effizient Indices / diskrete Logarithmen berechnen.

Ideen

1. Speichere nur Indices von Primzahlen.

Tafeln von Indices

Ziel. Wir wollen eine partielle Tafel benutzen und trotzdem (ziemlich) effizient Indices / diskrete Logarithmen berechnen.

Ideen

1. Speichere nur Indices von Primzahlen.

Dann:

Sei B eine ganze Zahl $< p$, $b := [B]_p$ gegeben. Was ist $\log_a(b)$?

Tafeln von Indices

Ziel. Wir wollen eine partielle Tafel benutzen und trotzdem (ziemlich) effizient Indices / diskrete Logarithmen berechnen.

Ideen

1. Speichere nur Indices von Primzahlen.

Dann:

Sei B eine ganze Zahl $< p$, $b := [B]_p$ gegeben. Was ist $\log_a(b)$?

Faktorisiere nun B (wie ?):

$$B = P_1 \cdots P_k \ .$$

Tafeln von Indices

Ziel. Wir wollen eine partielle Tafel benutzen und trotzdem (ziemlich) effizient Indices / diskrete Logarithmen berechnen.

Ideen

1. Speichere nur Indices von Primzahlen.

Dann:

Sei B eine ganze Zahl $< p$, $b := [B]_p$ gegeben. Was ist $\log_a(b)$?

Faktorisiere nun B (wie ?):

$$B = P_1 \cdots P_k \ .$$

Mit $p_i = [P_i]_p$:

$$\log_a(b) \equiv \log_a(p_1) + \cdots + \log_a(p_k) \pmod{p-1} \ .$$

Ideen zu Tafeln von Indices

2. Speichere nur Indices von Primzahlen unter einer gewissen Schranke $S < p$.

Ideen zu Tafeln von Indices

2. Speichere nur Indices von Primzahlen unter einer gewissen Schranke $S < p$.

Dann:
Sei B eine ganze Zahl $< p$, $b := [B]_p$. Was ist $\log_a(b)$?

Ideen zu Tafeln von Indices

2. Speichere nur Indices von Primzahlen unter einer gewissen Schranke $S < p$.

Dann:
Sei B eine ganze Zahl $< p$, $b := [B]_p$. Was ist $\log_a(b)$?

Betrachte den Repräsentant $C < p$ von $a^i b$ für $i = 1, 2, \ldots$ bis dieser in Primzahlen $< S$ faktorisiert:

$$C = P_1 \cdots P_k$$

Ideen zu Tafeln von Indices

2. Speichere nur Indices von Primzahlen unter einer gewissen Schranke $S < p$.

Dann:
Sei B eine ganze Zahl $< p$, $b := [B]_p$. Was ist $\log_a(b)$?

Betrachte den Repräsentant $C < p$ von $a^i b$ für $i = 1, 2, \ldots$ bis dieser in Primzahlen $< S$ faktorisiert:

$$C = P_1 \cdots P_k$$

Sei $c := a^i b$. Dann ist

$$i + \log_a(b) \equiv \log_a(c) \equiv \log_a(p_1) + \cdots + \log_a(p_k) \pmod{p-1}.$$

Tafeln von Indices

Sei eine Primzahl p und eine Primitivwurzel A gegeben. Wir interessieren uns für diskrete Logarithmen zur Basis $a := [A]_p$.

Herausforderung

Für eine Schranke $S < p$ berechne die entsprechende Tafel von Indices / "Logarithmentafel" für Primzahlen $< S$.

Tafeln von Indices

Sei eine Primzahl p und eine Primitivwurzel A gegeben. Wir interessieren uns für diskrete Logarithmen zur Basis $a := [A]_p$.

Herausforderung

Für eine Schranke $S < p$ berechne die entsprechende Tafel von Indices / "Logarithmentafel" für Primzahlen $< S$.

Begriffe

Die Primzahlen $< S$ bilden die sogenannte Faktorbasis.

Eine Zahl, die über der Faktorbasis faktorisiert, heißt glatt.

Indexkalkül

Die folgende Methode wurde von Maurice Kraitchik entwickelt. Sie findet sich in seinem Buch *Théorie des Nombres* von 1926.

Indexkalkül

Seien p, A und $S < p$ gegeben. Wir wollen die Tafel von Indices von Primzahlen $\leq S$ modulo p bezüglich A berechnen.

1. Nummeriere die Primzahlen $\leq S$: $P_1, P_2, \ldots$.

Indexkalkül

Seien p, A und $S < p$ gegeben. Wir wollen die Tafel von Indices von Primzahlen $\leq S$ modulo p bezüglich A berechnen.

1. Nummeriere die Primzahlen $\leq S$: $P_1, P_2, \ldots$.
2. Für $\ell = 1, 2, \ldots$:
   Versuche den Repräsentant $C < p$ von a^ℓ über S zu faktorisieren.
   Wenn
   $$C = P_1^{r_1} \cdots P_k^{r_k} :$$

Indexkalkül

Seien p, A und $S < p$ gegeben. Wir wollen die Tafel von Indices von Primzahlen $\leq S$ modulo p bezüglich A berechnen.

1. Nummeriere die Primzahlen $\leq S$: $P_1, P_2, \ldots$.
2. Für $\ell = 1, 2, \ldots$:
   Versuche den Repräsentant $C < p$ von a^ℓ über S zu faktorisieren.
   Wenn
   $$C = P_1^{r_1} \cdots P_k^{r_k} :$$
   $$[\quad \ell \equiv r_1 \log_a(p_1) + \cdots + r_k \log_a(p_k) \pmod{p-1} \quad]$$

Indexkalkül

Seien p, A und $S < p$ gegeben. Wir wollen die Tafel von Indices von Primzahlen $\leq S$ modulo p bezüglich A berechnen.

1. Nummeriere die Primzahlen $\leq S$: $P_1, P_2, \ldots$.
2. Für $\ell = 1, 2, \ldots$:

   Versuche den Repräsentant $C < p$ von a^ℓ über S zu faktorisieren.

   Wenn

   $$C = P_1^{r_1} \cdots P_k^{r_k} :$$

   $$[\quad \ell \equiv r_1 \log_a(p_1) + \cdots + r_k \log_a(p_k) \pmod{p-1} \quad]$$

   Speichere $(\ell, (r_1, \ldots, r_k))$ als Zeile einer "erweiterten Matrix" ab.

Indexkalkül

Seien p, A und $S < p$ gegeben. Wir wollen die Tafel von Indices von Primzahlen $\leq S$ modulo p bezüglich A berechnen.

1. Nummeriere die Primzahlen $\leq S$: $P_1, P_2, \ldots$.
2. Für $\ell = 1, 2, \ldots$:

   Versuche den Repräsentant $C < p$ von a^ℓ über S zu faktorisieren.

   Wenn

   $$C = P_1^{r_1} \cdots P_k^{r_k} :$$

   $$[\quad \ell \equiv r_1 \log_a(p_1) + \cdots + r_k \log_a(p_k) \pmod{p-1} \quad]$$

   Speichere $(\ell, (r_1, \ldots, r_k))$ als Zeile einer "erweiterten Matrix" ab.
3. Setze die Indices $\log_a(p_1), \ldots, \log_a(p_k)$ als Umbestimmte an, löse das lineare Gleichungssystem (modulo $p-1$).

Satz (Carl Pomerance, 1987). Das diskrete Logarithmusproblem in multiplikativen Gruppen von Primkörpern $\mathbf{F}_p$ kann in einer erwarteten Zeit von

$$\exp((\sqrt{2} + o(1)) \cdot \sqrt{\log(p) \cdot \log\log(p)})$$

gelöst werden.

Für Erweiterungskörper

Betrachte das DLP in $\mathbf{F}_{p^e}^*$ für p fest oder klein.

Für Erweiterungskörper

Betrachte das DLP in $\mathbf{F}_{p^e}^*$ für p fest oder klein.

Sei explizit $\mathbf{F}_{p^e}^* = \mathbf{F}_p[x]/(f)$.

Für Erweiterungskörper

Betrachte das DLP in $\mathbf{F}_{p^e}^*$ für p fest oder klein.

Sei explizit $\mathbf{F}_{p^e}^* = \mathbf{F}_p[x]/(f)$.

Nun: Ersetze ganze Zahlen durch Polynome.

Für Erweiterungskörper

Betrachte das DLP in $\mathbf{F}_{p^e}^*$ für p fest oder klein.

Sei explizit $\mathbf{F}_{p^e}^* = \mathbf{F}_p[x]/(f)$.

Nun: Ersetze ganze Zahlen durch Polynome.

Betrachte anstatt von

$$\mathbf{Z} \longrightarrow\!\!\!\!\!\rightarrow \mathbf{F}_p$$

$$A \longmapsto [A]_p$$

den Homomorphismus

$$\mathbf{F}_p[x] \longrightarrow\!\!\!\!\!\rightarrow \mathbf{F}_p[x]/(f)$$

$$G \longmapsto [G]_f \ .$$

Faktorisiere Polynome statt Zahlen ...

Für Erweiterungskörper

Stand bis ca. 2013:

Das ist ähnlich zu Methode für das klassische DLP, nur ein wenig schneller, weil man schneller (und leichter) Faktorisieren kann.

Für Erweiterungskörper

Stand bis ca. 2013:

Das ist ähnlich zu Methode für das klassische DLP, nur ein wenig schneller, weil man schneller (und leichter) Faktorisieren kann.

Heutzutage:

Für $\mathbf{F}_q$, die man passend darstellen kann ($\mathbf{F}_p[x]/(f)$ mit passendem f), so kann das DLP in einer erwarteten Zeit von

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

gelöst werden.

(Robert Granger, Thorsten Kleinjung, Jens Zumbrägel, 2015)

Zusammenfassung

Es gibt zwei Arten von Algorithmen für diskrete Logarithmenprobleme in endlichen Körpern:

- Generische Verfahren
- Relationensuch- und Lineare-Algebra-Verfahren = Indexkalkülverfahren

Zusammenfassung

Es gibt zwei Arten von Algorithmen für diskrete Logarithmenprobleme in endlichen Körpern:

- Generische Verfahren
- Relationensuch- und Lineare-Algebra-Verfahren = Indexkalkülverfahren

Laufzeiten

Zusammenfassung

Es gibt zwei Arten von Algorithmen für diskrete Logarithmenprobleme in endlichen Körpern:

- Generische Verfahren
- Relationensuch- und Lineare-Algebra-Verfahren = Indexkalkülverfahren

Laufzeiten

Generische Verfahren

ca. $\sqrt{\ell}$, wobei ℓ der größte Primteiler von ord(a) ist.

Zusammenfassung

Es gibt zwei Arten von Algorithmen für diskrete Logarithmenprobleme in endlichen Körpern:

- Generische Verfahren
- Relationensuch- und Lineare-Algebra-Verfahren = Indexkalkülverfahren

Laufzeiten

Generische Verfahren

ca. $\sqrt{\ell}$, wobei ℓ der größte Primteiler von ord(a) ist.

Indexkalkülverfahren

In $\mathbf{F}_q^*$: subexponentiell in $\log(q)$, (so gut wie) kein Vorteil durch kleine Ordnung von a.

Zusammenfassung

Es gibt zwei Arten von Algorithmen für diskrete Logarithmenprobleme in endlichen Körpern:

- Generische Verfahren
- Relationensuch- und Lineare-Algebra-Verfahren = Indexkalkülverfahren

Laufzeiten

Generische Verfahren

ca. $\sqrt{\ell}$, wobei ℓ der größte Primteiler von ord(a) ist.

Indexkalkülverfahren

In $\mathbf{F}_q^*$: subexponentiell in $\log(q)$, (so gut wie) kein Vorteil durch kleine Ordnung von a.

In $\mathbf{F}_{p^e}$, p fest oder klein: (ziemlich sicher) quasipolynomiell in e.

Generische Methoden

Keine direkten Rekorde für endliche Körper, aber in elliptischen Kurven

dort: 117 bit

(Daniel Bernstein, Susanne Engels, Tanja Lange, Rubin Niederhagen, Christoph Paar, Peter Schwabe, Ralf Zimmermann, 2016)

Rekorde

Generische Methoden

Keine direkten Rekorde für endliche Körper, aber in elliptischen Kurven

dort: 117 bit

(Daniel Bernstein, Susanne Engels, Tanja Lange, Rubin Niederhagen, Christoph Paar, Peter Schwabe, Ralf Zimmermann, 2016)

Indexkalkül

In Primkörpern: 768 bit mit dem sogenannten Zahlkörpersieb

(Thorsten Kleinjung, C.D., Arjen Lenstra, Christine Priplata, Colin Stahlke, 2016)

In Erweiterungskörpern: z.B. (insbesondere) in $\mathbf{F}_{2^{1729}}$ (mit Primzahl 1729)

(Kleinjung, 2014)

Variante von Indexkalkül

Seien p prim, $a, b \in \mathbf{F}_p^*$ mit $b \in \langle a \rangle$ gegeben.

Ziel. Berechne nur den einen diskreten Logarithmus $\log_a(b)$!

Variante von Indexkalkül

Seien p prim, $a, b \in \mathbf{F}_p^*$ mit $b \in \langle a \rangle$ gegeben.

Ziel. Berechne nur den einen diskreten Logarithmus $\log_a(b)$!

1. Wähle eine Glattheitsschranke $S < p$, nummeriere die Primzahlen $P_1, P_2, \ldots, P_k < S$.

Variante von Indexkalkül

Seien p prim, $a, b \in \mathbf{F}_p^*$ mit $b \in \langle a \rangle$ gegeben.

Ziel. Berechne nur den einen diskreten Logarithmus $\log_a(b)$!

1. Wähle eine Glattheitsschranke $S < p$, nummeriere die Primzahlen $P_1, P_2, \ldots, P_k < S$.
2. Berechne Relationen

$$a^\alpha b^\beta = p_1^{r_1} \cdots p_k^{r_k} :$$

(Wähle α, β zufällig, dann wie zuvor.)

$$[\, \alpha + \beta \log_a(b) \equiv r_1 \log(p_1) + \cdots + r_k \log(p_k) \pmod{p-1} \,]$$

Speichere diese in $(\underline{\alpha}, \underline{\beta}, R)$ ab.

Variante von Indexkalkül

Seien p prim, $a, b \in \mathbf{F}_p^*$ mit $b \in \langle a \rangle$ gegeben.

Ziel. Berechne nur den einen diskreten Logarithmus $\log_a(b)$!

1. Wähle eine Glattheitsschranke $S < p$, nummeriere die Primzahlen $P_1, P_2, \ldots, P_k < S$.
2. Berechne Relationen

$$a^\alpha b^\beta = p_1^{r_1} \cdots p_k^{r_k} :$$

(Wähle α, β zufällig, dann wie zuvor.)

$$[\ \alpha + \beta \log_a(b) \equiv r_1 \log(p_1) + \cdots + r_k \log(p_k) \pmod{p-1}\ ]$$

Speichere diese in $(\underline{\alpha}, \underline{\beta}, R)$ ab.

3. Berechne v über $\mathbf{Z}/(p-1)\mathbf{Z}$ mit $\underline{v}R = 0$.

$$[\ (\sum_i \alpha_i v_i) + (\sum_i \beta_i v_i) \cdot [\log_a(b)]_{p-1} = 0\ ]$$

Variante von Indexkalkül

Seien p prim, $a, b \in \mathbf{F}_p^*$ mit $b \in \langle a \rangle$ gegeben.

Ziel. Berechne nur den einen diskreten Logarithmus $\log_a(b)$!

1. Wähle eine Glattheitsschranke $S < p$, nummeriere die Primzahlen $P_1, P_2, \ldots, P_k < S$.
2. Berechne Relationen

$$a^\alpha b^\beta = p_1^{r_1} \cdots p_k^{r_k} :$$

(Wähle α, β zufällig, dann wie zuvor.)

$$[\, \alpha + \beta \log_a(b) \equiv r_1 \log(p_1) + \cdots + r_k \log(p_k) \pmod{p-1} \,]$$

Speichere diese in $(\underline{\alpha}, \underline{\beta}, R)$ ab.

3. Berechne v über $\mathbf{Z}/(p-1)\mathbf{Z}$ mit $\underline{v}R = 0$.

$$[\, (\sum_i \alpha_i v_i) + (\sum_i \beta_i v_i) \cdot [\log_a(b)]_{p-1} = 0 \,]$$

4. Gib $-\frac{\sum_i \alpha_i v_i}{\sum_i \beta_i v_i} \in \mathbf{Z}/(p-1)\mathbf{Z}$ aus, wenn möglich.

Faktorisierung

Faktorisierung

Teil 1: Fermat-Faktorisierung mit Faktorbasis

Fermat-Faktorisierung

Sei $N \in \mathbf{N}$ nicht prim gegeben.

Ziel. Finde einen nicht-trivialen Teiler von N.

Fermat-Faktorisierung

Sei $N \in \mathbf{N}$ nicht prim gegeben.

Ziel. Finde einen nicht-trivialen Teiler von N.

Angenommen wir haben

$$X^2 \equiv Y^2 \mod N$$

Fermat-Faktorisierung

Sei $N \in \mathbf{N}$ nicht prim gegeben.

Ziel. Finde einen nicht-trivialen Teiler von N.

Angenommen wir haben

$$X^2 \equiv Y^2 \mod N$$

Dann ist:

$$N \mid (X - Y)(X + Y)$$

Wenn nun X und Y "irgendwie zufällig" sind, liegt nahe, dass $\mathrm{ggT}(N, X - Y)$ ein nicht-trivialer Teiler von N ist.

Fermat-Faktorisierung

Sei $N \in \mathbf{N}$ nicht prim gegeben.

Ziel. Finde einen nicht-trivialen Teiler von N.

Angenommen wir haben

$$X^2 \equiv Y^2 \mod N$$

Dann ist:

$$N \mid (X - Y)(X + Y)$$

Wenn nun X und Y "irgendwie zufällig" sind, liegt nahe, dass $\mathrm{ggT}(N, X - Y)$ ein nicht-trivialer Teiler von N ist.

Fermat. Betrachte $X = \lceil \sqrt{N} \rceil, \lceil \sqrt{N} \rceil + 1, \ldots$, hierzu $X^2 - N$, bis dies ein Quadrat ist.

Fermat-Faktorisierung mit Faktorbasis

1. Wähle eine Glattheitsschranke $S < p$, nummeriere die Primzahlen $P_1, P_2, \ldots, P_k < S$.

Fermat-Faktorisierung mit Faktorbasis

1. Wähle eine Glattheitsschranke $S < p$, nummeriere die Primzahlen $P_1, P_2, \ldots, P_k < S$.
2. Wiederhole:
   Wähle $X < N$ zufällig.
   Sei $C < N$ mit $C \equiv X^2 \bmod N$ (d.h. $[C]_N = [X^2]_N$).
   Versuche, C über der Faktorbasis zu faktorisieren.
   Wenn $C = P_1^{r_1} \cdots P_k^{r_k}$:
   Speichere $(X; r_1, \ldots, r_k)$ als Zeile einer "erweiterten Matrix".

Fermat-Faktorisierung mit Faktorbasis

1. Wähle eine Glattheitsschranke $S < p$, nummeriere die Primzahlen $P_1, P_2, \ldots, P_k < S$.
2. Wiederhole:
   Wähle $X < N$ zufällig.
   Sei $C < N$ mit $C \equiv X^2 \bmod N$ (d.h. $[C]_N = [X^2]_N$).
   Versuche, C über der Faktorbasis zu faktorisieren.
   Wenn $C = P_1^{r_1} \cdots P_k^{r_k}$:
   Speichere $(X; r_1, \ldots, r_k)$ als Zeile einer "erweiterten Matrix".
   Bis $k + 1$ Zeilen vorhanden sind.

Fermat-Faktorisierung mit Faktorbasis

1. Wähle eine Glattheitsschranke $S < p$, nummeriere die Primzahlen $P_1, P_2, \ldots, P_k < S$.
2. Wiederhole:
   Wähle $X < N$ zufällig.
   Sei $C < N$ mit $C \equiv X^2 \bmod N$ (d.h. $[C]_N = [X^2]_N$).
   Versuche, C über der Faktorbasis zu faktorisieren.
   Wenn $C = P_1^{r_1} \cdots P_k^{r_k}$:
   Speichere $(X; r_1, \ldots, r_k)$ als Zeile einer "erweiterten Matrix".
   Bis $k + 1$ Zeilen vorhanden sind.
   Erhalte einen Vektor $(X_i)_i$ und eine Matrix $R = (r_{i,j})_{i,j}$.

Fermat-Faktorisierung mit Faktorbasis

1. Wähle eine Glattheitsschranke $S < p$, nummeriere die Primzahlen $P_1, P_2, \ldots, P_k < S$.
2. Wiederhole:
   Wähle $X < N$ zufällig.
   Sei $C < N$ mit $C \equiv X^2 \bmod N$ (d.h. $[C]_N = [X^2]_N$).
   Versuche, C über der Faktorbasis zu faktorisieren.
   Wenn $C = P_1^{r_1} \cdots P_k^{r_k}$:
   Speichere $(X; r_1, \ldots, r_k)$ als Zeile einer "erweiterten Matrix".
   Bis $k+1$ Zeilen vorhanden sind.
   Erhalte einen Vektor $(X_i)_i$ und eine Matrix $R = (r_{i,j})_{i,j}$.
3. Berechne $\underline{v} \in \{0,1\}^{k+1}$ mit $\underline{v}R \equiv 0 \mod 2$.

Fermat-Faktorisierung mit Faktorbasis

1. Wähle eine Glattheitsschranke $S < p$, nummeriere die Primzahlen $P_1, P_2, \ldots, P_k < S$.
2. Wiederhole:
   Wähle $X < N$ zufällig.
   Sei $C < N$ mit $C \equiv X^2 \bmod N$ (d.h. $[C]_N = [X^2]_N$).
   Versuche, C über der Faktorbasis zu faktorisieren.
   Wenn $C = P_1^{r_1} \cdots P_k^{r_k}$:
   Speichere $(X; r_1, \ldots, r_k)$ als Zeile einer "erweiterten Matrix".
   Bis $k+1$ Zeilen vorhanden sind.
   Erhalte einen Vektor $(X_i)_i$ und eine Matrix $R = (r_{i,j})_{i,j}$.
3. Berechne $\underline{v} \in \{0,1\}^{k+1}$ mit $\underline{v}R \equiv 0 \mod 2$.

$$\left[\quad \left(\prod_i X_i^{v_i}\right)^2 \equiv \prod_j P_j^{\sum_i v_i r_{i,j}} = \left(\prod_j P_j^{\sum_i v_i r_{i,j}/2}\right)^2 \quad \right]$$

Fermat-Faktorisierung mit Faktorbasis

1. Wähle eine Glattheitsschranke $S < p$, nummeriere die Primzahlen $P_1, P_2, \ldots, P_k < S$.
2. Wiederhole:
   Wähle $X < N$ zufällig.
   Sei $C < N$ mit $C \equiv X^2 \bmod N$ (d.h. $[C]_N = [X^2]_N$).
   Versuche, C über der Faktorbasis zu faktorisieren.
   Wenn $C = P_1^{r_1} \cdots P_k^{r_k}$:
   Speichere $(X; r_1, \ldots, r_k)$ als Zeile einer "erweiterten Matrix".
   Bis $k+1$ Zeilen vorhanden sind.
   Erhalte einen Vektor $(X_i)_i$ und eine Matrix $R = (r_{i,j})_{i,j}$.
3. Berechne $\underline{v} \in \{0,1\}^{k+1}$ mit $\underline{v}R \equiv 0 \mod 2$.

$$\left[\quad \left(\prod_i X_i^{v_i}\right)^2 \equiv \prod_j P_j^{\sum_i v_i r_{i,j}} = \left(\prod_j P_j^{\sum_i v_i r_{i,j}/2}\right)^2 \quad \right]$$

4. Wie Fermat-Faktorisierung.

Fermat-Faktorisierung mit Faktorbasis

Satz (Carl Pomerance, 1987). Eine natürliche Zahl N kann in einer erwarteten Zeit von

$$\exp((\sqrt{2} + o(1)) \cdot \sqrt{\log(p) \cdot \log\log(p)})$$

faktorisiert werden.

Fermat-Faktorisierung mit Faktorbasis

Satz (Carl Pomerance, 1987). Eine natürliche Zahl N kann in einer erwarteten Zeit von

$$\exp((\sqrt{2} + o(1)) \cdot \sqrt{\log(p) \cdot \log\log(p)})$$

faktorisiert werden.

Kann verbessert werden zu:

Satz (Henrik Lenstra & Carl Pomerance, 1991). Eine natürliche Zahl N kann in einer erwarteten Zeit von

$$\exp((1 + o(1)) \cdot \sqrt{\log(p) \cdot \log\log(p)})$$

faktorisiert werden.

Rekord

"RSA 768"

(Thorsten Kleinjung, Kazumaro Aoki, Jens Franke, Arjen Lenstra, Emmanuel Thomé, Joppe Bos, Pierrick Gaudry, Alexander Kruppa, Peter Montgomery, Dag Osvik, Herman te Riele, Andrey Timofeev, Paul Zimmermann)

und weitere Rekord für größere "spezielle Zahlen".

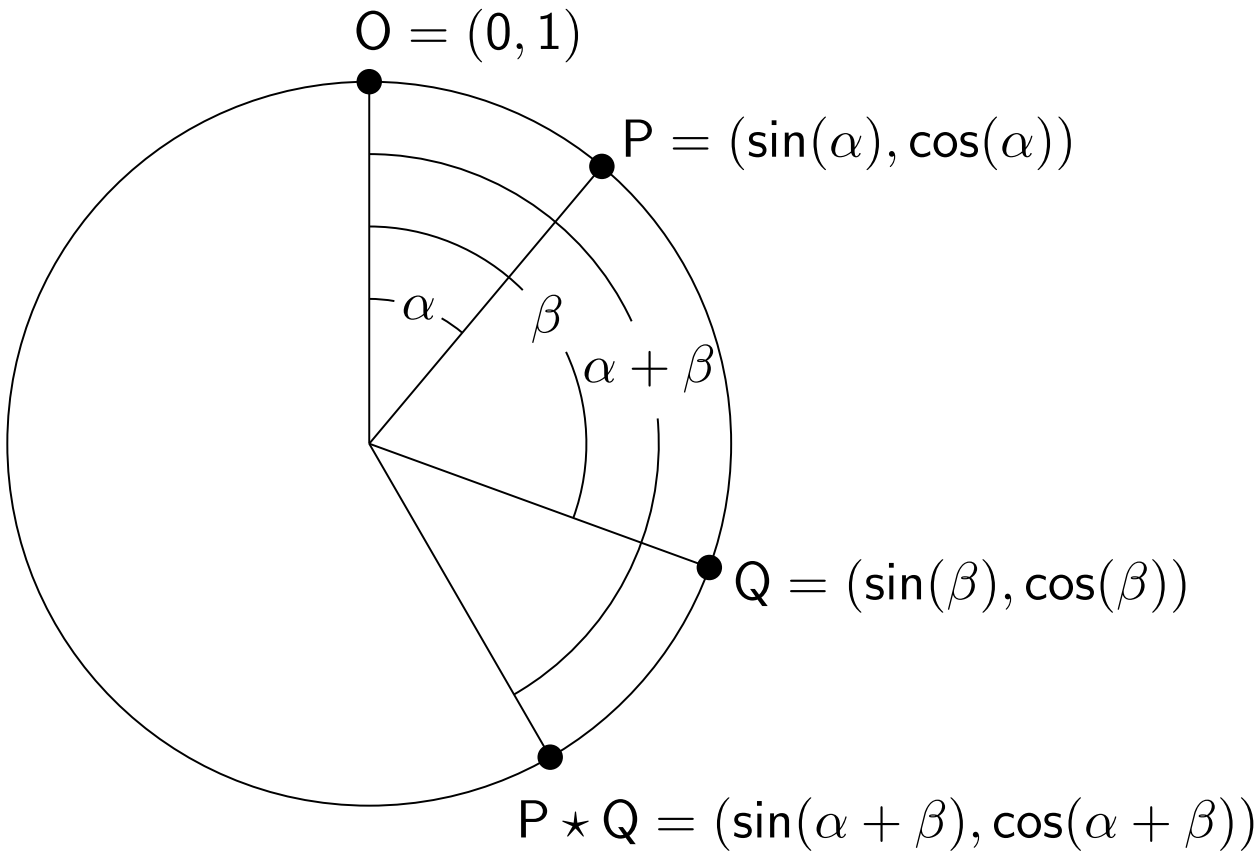
Also: 768 bit für DL und Faktorisieren.

Elliptische Kurven

in Edwards-Form

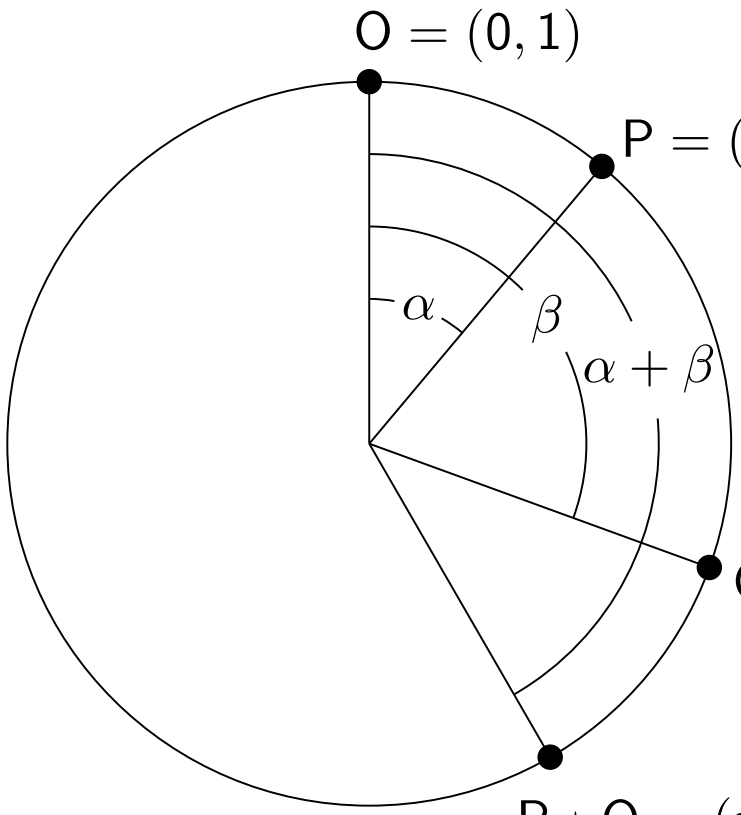
Der Kreis

gegeben durch $x^2 + y^2 = 1$



Der Kreis

gegeben durch $x^2 + y^2 = 1$



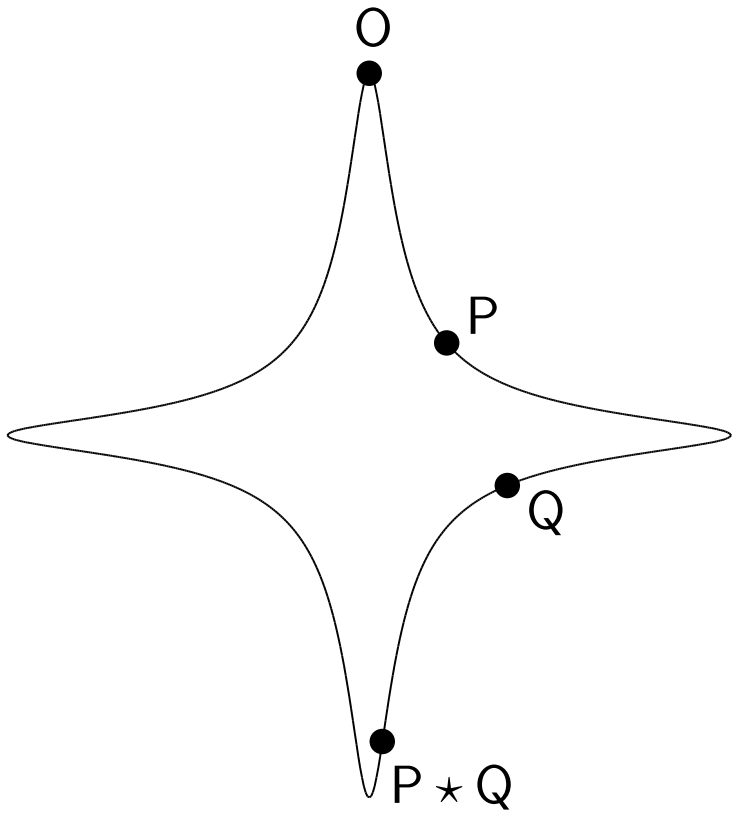
mit $R = P \star Q$:

$$x_R = x_P x_Q + x_Q x_P$$
$$y_R = y_P y_Q - x_P x_Q$$

Elliptische Kurven

Die elliptische Kurve gegeben durch

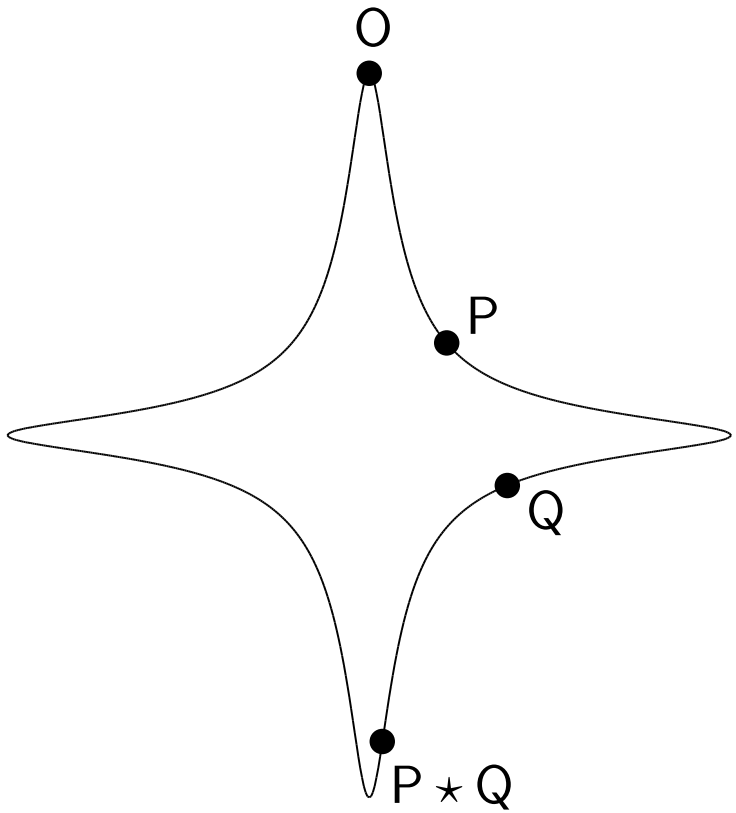
$$x^2 + y^2 = 1 - 300x^2y^2 \ .$$



Elliptische Kurven

Die elliptische Kurve gegeben durch

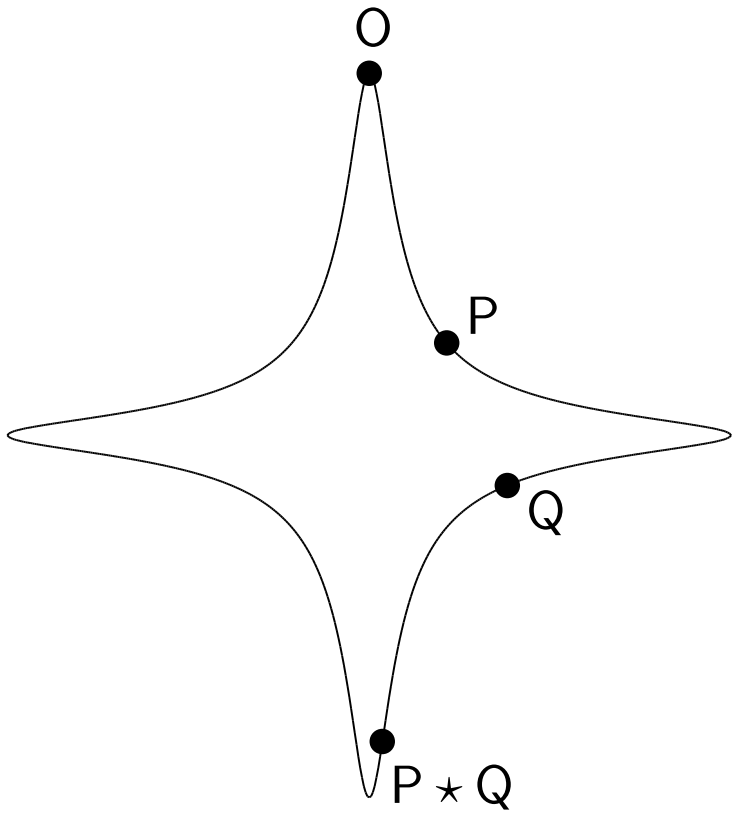
$x^2 + y^2 = 1 + dx^2y^2$, $d < 0$.



Elliptische Kurven

Die elliptische Kurve gegeben durch

$x^2 + y^2 = 1 + dx^2y^2$, $d < 0$.



mit $R = P \star Q$:

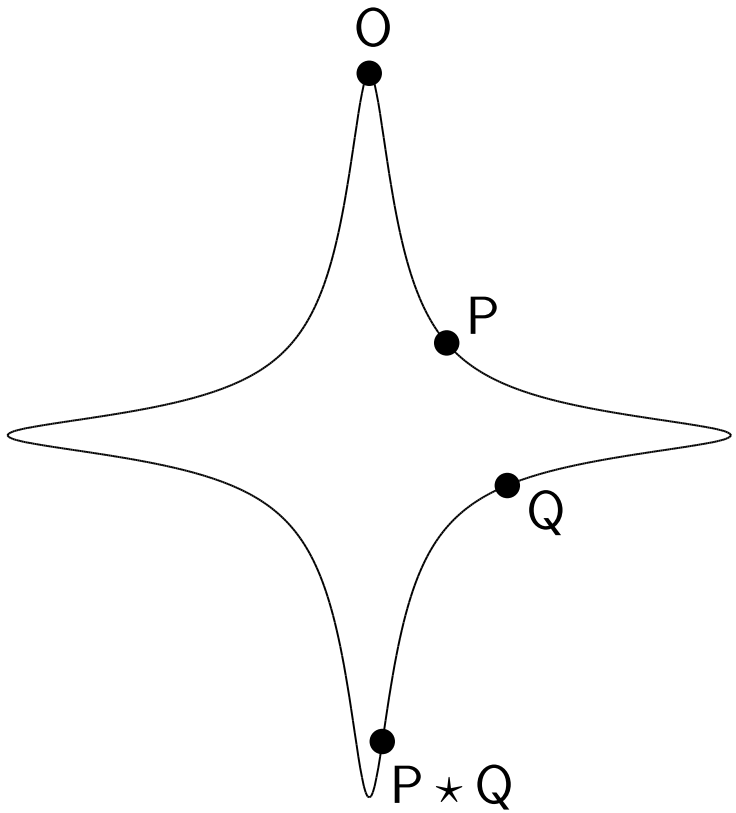
$$x_R = \frac{x_P x_Q + x_Q x_P}{1 + d x_P x_Q y_P y_Q}$$

$$y_R = \frac{y_P y_Q - x_P x_Q}{1 - d x_P x_Q y_P y_Q}$$

Elliptische Kurven

Die elliptische Kurve gegeben durch

$x^2 + y^2 = 1 + dx^2y^2$, $d < 0$.



mit $R = P \star Q$:

$$x_R = \frac{x_P x_Q + x_Q x_P}{1 + d x_P x_Q y_P y_Q}$$

$$y_R = \frac{y_P y_Q - x_P x_Q}{1 - d x_P x_Q y_P y_Q}$$

d ist kein Quadrat.

Quadrate in endlichen Körpern

Ersetze $\mathbf{R}$ durch endlichen Körper $\mathbf{F}_q$!

Quadrate in endlichen Körpern

Ersetze $\mathbf{R}$ durch endlichen Körper $\mathbf{F}_q$!

Welche Elemente sind Quadrate?

Quadrate in endlichen Körpern

Ersetze $\mathbf{R}$ durch endlichen Körper $\mathbf{F}_q$!

Welche Elemente sind Quadrate?

Erstmal 0 ...

Quadrate in endlichen Körpern

Ersetze $\mathbf{R}$ durch endlichen Körper $\mathbf{F}_q$!

Welche Elemente sind Quadrate?

Erstmal 0 ...

Sei a ein Erzeuger ($\mathrm{ord}(a) = q - 1$).

Quadrate in endlichen Körpern

Ersetze $\mathbf{R}$ durch endlichen Körper $\mathbf{F}_q$!

Welche Elemente sind Quadrate?

Erstmal 0 ...

Sei a ein Erzeuger ($\mathrm{ord}(a) = q - 1$).

- Die Elemente a^{2k} sind Quadrate.
- Dies sind alle Quadrate in $\mathbf{F}_q^*$.

Quadrate in endlichen Körpern

Ersetze $\mathbf{R}$ durch endlichen Körper $\mathbf{F}_q$!

Welche Elemente sind Quadrate?

Erstmal 0 ...

Sei a ein Erzeuger ($\mathrm{ord}(a) = q - 1$).

- Die Elemente a^{2k} sind Quadrate.
- Dies sind alle Quadrate in $\mathbf{F}_q^*$.

Denn. Die zweite Aussage besagt:

Quadrate in endlichen Körpern

Ersetze $\mathbf{R}$ durch endlichen Körper $\mathbf{F}_q$!

Welche Elemente sind Quadrate?

Erstmal 0 ...

Sei a ein Erzeuger ($\mathrm{ord}(a) = q - 1$).

- Die Elemente a^{2k} sind Quadrate.
- Dies sind alle Quadrate in $\mathbf{F}_q^*$.

Denn. Die zweite Aussage besagt:

Sei $d \in \mathbf{F}_q^*$ ein Quadrat. Dann ist $d = c^2$ für ein c.

Quadrate in endlichen Körpern

Ersetze $\mathbf{R}$ durch endlichen Körper $\mathbf{F}_q$!

Welche Elemente sind Quadrate?

Erstmal 0 ...

Sei a ein Erzeuger ($\mathrm{ord}(a) = q - 1$).

- Die Elemente a^{2k} sind Quadrate.
- Dies sind alle Quadrate in $\mathbf{F}_q^*$.

Denn. Die zweite Aussage besagt:

Sei $d \in \mathbf{F}_q^*$ ein Quadrat. Dann ist $d = c^2$ für ein c.

Sei dies der Fall. Da a ein Erzeuger ist, ist $c = a^k$ für ein k.

Quadrate in endlichen Körpern

Ersetze $\mathbf{R}$ durch endlichen Körper $\mathbf{F}_q$!

Welche Elemente sind Quadrate?

Erstmal 0 ...

Sei a ein Erzeuger ($\mathrm{ord}(a) = q - 1$).

- Die Elemente a^{2k} sind Quadrate.
- Dies sind alle Quadrate in $\mathbf{F}_q^*$.

Denn. Die zweite Aussage besagt:

Sei $d \in \mathbf{F}_q^*$ ein Quadrat. Dann ist $d = c^2$ für ein c.

Sei dies der Fall. Da a ein Erzeuger ist, ist $c = a^k$ für ein k.

Damit $d = a^{2k}$.

Quadrate in endlichen Körpern

Ersetze $\mathbf{R}$ durch endlichen Körper $\mathbf{F}_q$!

Welche Elemente sind Quadrate?

Erstmal 0.

Sei a ein Erzeuger ($\mathrm{ord}(a) = q - 1$).

- Die Elemente a^{2k} sind Quadrate.
- Dies sind alle Quadrate in $\mathbf{F}_q^*$.

Quadrate in endlichen Körpern

Ersetze $\mathbf{R}$ durch endlichen Körper $\mathbf{F}_q$!

Welche Elemente sind Quadrate?

Erstmal 0.

Sei a ein Erzeuger ($\mathrm{ord}(a) = q - 1$).

- Die Elemente a^{2k} sind Quadrate.
- Dies sind alle Quadrate in $\mathbf{F}_q^*$.

Da a Erzeuger mit gerader Ordnung:

$\mathbf{F}_q$ teilt sich auf in:

- 0

Quadrate in endlichen Körpern

Ersetze $\mathbf{R}$ durch endlichen Körper $\mathbf{F}_q$!

Welche Elemente sind Quadrate?

Erstmal 0.

Sei a ein Erzeuger ($\mathrm{ord}(a) = q - 1$).

- Die Elemente a^{2k} sind Quadrate.
- Dies sind alle Quadrate in $\mathbf{F}_q^*$.

Da a Erzeuger mit gerader Ordnung:

$\mathbf{F}_q$ teilt sich auf in:

- 0
- Die Quadrate a^{2k} ($\frac{q-1}{2}$ viele)

Quadrate in endlichen Körpern

Ersetze $\mathbf{R}$ durch endlichen Körper $\mathbf{F}_q$!

Welche Elemente sind Quadrate?

Erstmal 0.

Sei a ein Erzeuger ($\mathrm{ord}(a) = q - 1$).

- Die Elemente a^{2k} sind Quadrate.
- Dies sind alle Quadrate in $\mathbf{F}_q^*$.

Da a Erzeuger mit gerader Ordnung:

$\mathbf{F}_q$ teilt sich auf in:

- 0
- Die Quadrate a^{2k} ($\frac{q-1}{2}$ viele)
- Die Nicht-Quadrate a^{2k+1} ($\frac{q-1}{2}$ viele)

Quadrate in endlichen Körpern

Oder so:

Für $d \in \mathbf{F}_q$ sind äquivalent:

- d ist Quadrat
- $d^{\frac{q-1}{2}} = 1$
- $\mathrm{ord}(d) \mid \frac{q-1}{2}$

Quadrate in endlichen Körpern

Oder so:

Für $d \in \mathbf{F}_q$ sind äquivalent:

- d ist Quadrat
- $d^{\frac{q-1}{2}} = 1$
- $\mathrm{ord}(d) \mid \frac{q-1}{2}$

Algorithmisch einfach!

Elliptische Kurven

Sei K ein beliebiger Körper mit $1_K + 1_K \neq 0_K$.

Für d ein Nicht-Quadrat haben wir die

(Punktgruppe der) elliptischen Kurve gegeben durch

$$x^2 + y^2 = 1 + dx^2y^2 \ :$$

$$\{P = (x_P, y_P) \in K^2 \mid x_P^2 + y_p^2 = 1 + dx_P^2y_P^2\}$$

mit dem neutralen Element $O = (0, 1)$.

Elliptische Kurven

Sei K ein beliebiger Körper mit $1_K + 1_K \neq 0_K$.

Für d ein Nicht-Quadrat haben wir die

(Punktgruppe der) elliptischen Kurve gegeben durch

$$x^2 + y^2 = 1 + dx^2y^2 \ :$$

$$\{P = (x_P, y_P) \in K^2 \mid x_P^2 + y_p^2 = 1 + dx_P^2y_P^2\}$$

mit dem neutralen Element $O = (0, 1)$.

Typische Bezeichnung: $E(K)$.

Elliptische Kurven

Sei K ein beliebiger Körper mit $1_K + 1_K \neq 0_K$.

Für d ein Nicht-Quadrat haben wir die

(Punktgruppe der) elliptischen Kurve gegeben durch

$$x^2 + y^2 = 1 + dx^2y^2 \ :$$

$$\{P = (x_P, y_P) \in K^2 \mid x_P^2 + y_p^2 = 1 + dx_P^2y_P^2\}$$

mit dem neutralen Element $O = (0, 1)$.

Typische Bezeichnung: $E(K)$.

Für $d > 0, d \neq 1$ geht's auch.

Dann bekommt man aber Spezialfälle in der Additionsformel.

Elliptische Kurven

Die elliptische Kurve E/K zu der Gleichung

$$x^2 + y^2 = 1 + dx^2y^2$$

besteht aus allen Gruppen $E(L)$ für endliche Erweiterungskörper $L|K$.

Elliptische Kurven

Die elliptische Kurve E/K zu der Gleichung

$$x^2 + y^2 = 1 + dx^2y^2$$

besteht aus allen Gruppen $E(L)$ für endliche Erweiterungskörper $L|K$.

Beachte hier: Für Erweiterung $L|K$ (also $K \subseteq L$) ist auch $E(K) \subseteq E(L)$.

Für $K = \mathbf{F}_q$: Nicht nur $E(\mathbf{F}_q)$, sondern auch $E(\mathbf{F}_{q^e})$ für alle $e \in \mathbf{N}$.

Elliptische Kurven

Sei weiterhin $1_K + 1_K \neq 0_K$.

Elliptische Kurven

Sei weiterhin $1_K + 1_K \neq 0_K$.

Dies waren elliptische Kurven in Edwards-Form.

Elliptische Kurven

Sei weiterhin $1_K + 1_K \neq 0_K$.

Dies waren elliptische Kurven in Edwards-Form.

Man kann elliptische Kurven durch andere Gleichungen beschreiben.

Elliptische Kurven

Sei weiterhin $1_K + 1_K \neq 0_K$.

Dies waren elliptische Kurven in Edwards-Form.

Man kann elliptische Kurven durch andere Gleichungen beschreiben.

Insbesondere: Elliptische Kurven in Weierstraß-Form, gegeben durch

$$y^2 = f(x)$$

mit f von Grad 3 ohne mehrfache Nullstellen.

Elliptische Kurven

Sei weiterhin $1_K + 1_K \neq 0_K$.

Dies waren elliptische Kurven in Edwards-Form.

Man kann elliptische Kurven durch andere Gleichungen beschreiben.

Insbesondere: Elliptische Kurven in Weierstraß-Form, gegeben durch

$$y^2 = f(x)$$

mit f von Grad 3 ohne mehrfache Nullstellen.

(Und = "Punkt im Unendlichen")

Elliptische Kurven

Sei weiterhin $1_K + 1_K \neq 0_K$.

Dies waren elliptische Kurven in Edwards-Form.

Man kann elliptische Kurven durch andere Gleichungen beschreiben.

Insbesondere: Elliptische Kurven in Weierstraß-Form, gegeben durch

$$y^2 = f(x)$$

mit f von Grad 3 ohne mehrfache Nullstellen.

(Und = "Punkt im Unendlichen")

Jede Kurve in Edwards-Form ist isomorph zu einer in Weierstraß-Form, aber

umgekehrt geht's nicht immer ...

Die Gruppenordnung

Es sei $E/\mathbf{F}_q$ eine elliptische Kurve.

Satz (Satz von Helmut Hasse, 1936). Es gilt

$$|\#E(\mathbf{F}_q) - (q+1)| \leq 2\sqrt{q}\ .$$

Die Gruppenordnung

Es sei $E/\mathbf{F}_q$ eine elliptische Kurve.

Satz (Satz von Helmut Hasse, 1936). Es gilt

$$|\#E(\mathbf{F}_q) - (q+1)| \leq 2\sqrt{q}\ .$$

Beruht auf einer Formel, die auch $\#E(\mathbf{F}_q)$ und $\#E(\mathbf{F}_{q^e})$ verbindet.

Die Gruppenordnung

Es sei $E/\mathbf{F}_q$ eine elliptische Kurve.

Satz (Satz von Helmut Hasse, 1936). Es gilt

$$|\#E(\mathbf{F}_q) - (q+1)| \leq 2\sqrt{q}\ .$$

Beruht auf einer Formel, die auch $\#E(\mathbf{F}_q)$ und $\#E(\mathbf{F}_{q^e})$ verbindet.

Satz (von René Schoof, 1985) Die Gruppenordnung von $E(\mathbf{F}_q)$ kann man in polynomieller Zeit berechnen (Schoof Algorithmus).

Das Elliptische Kurven Diskrete Logarithmusproblem

Idee (Victor Miller & Neal Koblitz, ca. 1985). Für elliptische Kurven geht Indexkalkül nicht.

Wenn das stimmt:

Für elliptische Kurven über $\mathbf{F}_q$ mit q von 256 bit und Gruppenordung der Form $\ell \cdot c$ mit ℓ Primzahl, $c \leq 4$ ist DLP super-sicher.

Das Elliptische Kurven Diskrete Logarithmusproblem

Idee (Victor Miller & Neal Koblitz, ca. 1985). Für elliptische Kurven geht Indexkalkül nicht.

Wenn das stimmt:

Für elliptische Kurven über $\mathbf{F}_q$ mit q von 256 bit und Gruppenordung der Form $\ell \cdot c$ mit ℓ Primzahl, $c \leq 4$ ist DLP super-sicher.

Aber es gibt dann doch angreifbare Kurven, insbesondere:

Das Elliptische Kurven Diskrete Logarithmusproblem

Idee (Victor Miller & Neal Koblitz, ca. 1985). Für elliptische Kurven geht Indexkalkül nicht.

Wenn das stimmt:

Für elliptische Kurven über $\mathbf{F}_q$ mit q von 256 bit und Gruppenordung der Form $\ell \cdot c$ mit ℓ Primzahl, $c \leq 4$ ist DLP super-sicher.

Aber es gibt dann doch angreifbare Kurven, insbesondere:

- Für p prim, $\#E(\mathbf{F}_p) = p$ für DLP in $E(\mathbf{F}_p)$ (praktisch)

Das Elliptische Kurven Diskrete Logarithmusproblem

Idee (Victor Miller & Neal Koblitz, ca. 1985). Für elliptische Kurven geht Indexkalkül nicht.

Wenn das stimmt:

Für elliptische Kurven über $\mathbf{F}_q$ mit q von 256 bit und Gruppenordung der Form $\ell \cdot c$ mit ℓ Primzahl, $c \leq 4$ ist DLP super-sicher.

Aber es gibt dann doch angreifbare Kurven, insbesondere:

- Für p prim, $\#E(\mathbf{F}_p) = p$ für DLP in $E(\mathbf{F}_p)$ (praktisch)
- Für q Primpotenz, $\#E(\mathbf{F}_q) = q - 1$ für DLP in $E(\mathbf{F}_q)$ (pratisch).

Das Elliptische Kurven Diskrete Logarithmusproblem

Idee (Victor Miller & Neal Koblitz, ca. 1985). Für elliptische Kurven geht Indexkalkül nicht.

Wenn das stimmt:

Für elliptische Kurven über $\mathbf{F}_q$ mit q von 256 bit und Gruppenordung der Form $\ell \cdot c$ mit ℓ Primzahl, $c \leq 4$ ist DLP super-sicher.

Aber es gibt dann doch angreifbare Kurven, insbesondere:

- Für p prim, $\#E(\mathbf{F}_p) = p$ für DLP in $E(\mathbf{F}_p)$ (praktisch)
- Für q Primpotenz, $\#E(\mathbf{F}_q) = q - 1$ für DLP in $E(\mathbf{F}_q)$ (pratisch).
- Für bestimmte Kombinationen von q Primpotenz und $e \geq 3$ für DLP in $E(\mathbf{F}_{q^e})$ (theoretisch und teilweise praktisch).

Das Elliptische Kurven Diskrete Logarithmusproblem

Idee (Victor Miller & Neal Koblitz, ca. 1985). Für elliptische Kurven geht Indexkalkül nicht.

Wenn das stimmt:

Für elliptische Kurven über $\mathbf{F}_q$ mit q von 256 bit und Gruppenordung der Form $\ell \cdot c$ mit ℓ Primzahl, $c \leq 4$ ist DLP super-sicher.

Aber es gibt dann doch angreifbare Kurven, insbesondere:

- Für p prim, $\#E(\mathbf{F}_p) = p$ für DLP in $E(\mathbf{F}_p)$ (praktisch)
- Für q Primpotenz, $\#E(\mathbf{F}_q) = q - 1$ für DLP in $E(\mathbf{F}_q)$ (pratisch).
- Für bestimmte Kombinationen von q Primpotenz und $e \geq 3$ für DLP in $E(\mathbf{F}_{q^e})$ (theoretisch und teilweise praktisch).

Und Gefahr durch Quantencomputer.

Faktorisierung

Faktorisierung

Teil 2: Faktorisierung mit elliptischen Kurven

Vorbemerkung

Sei S eine Glattheitsschranke, $P_1, \ldots, P_k$ die Primzahlen $< S$.

Eine natürliche Zahl R heißt S-potenzglatt, falls

$$R = \prod_i P_i^{r_i}$$

mit $P_i^{r_i} \leq S$, d.h. $r_i \leq \lfloor \log_{P_i}(S) \rfloor$.

Vorbemerkung

Sei S eine Glattheitsschranke, $P_1, \ldots, P_k$ die Primzahlen $< S$.

Eine natürliche Zahl R heißt S-potenzglatt, falls

$$R = \prod_i P_i^{r_i}$$

mit $P_i^{r_i} \leq S$, d.h. $r_i \leq \lfloor \log_{P_i}(S) \rfloor$.

Oder:

$$R \mid \prod_i P_i^{\lfloor \log_{P_i}(S) \rfloor}$$

Vorbemerkung

Sei $G = (G, +)$ eine endliche abelsche Gruppe, $g \in G$.

Vorbemerkung

Sei $G = (G, +)$ eine endliche abelsche Gruppe, $g \in G$.

Es ist

$$\mathrm{ord}(g) \cdot g = O_G$$

Vorbemerkung

Sei $G = (G, +)$ eine endliche abelsche Gruppe, $g \in G$.

Es ist

$$\mathrm{ord}(g) \cdot g = O_G$$

Sei nun $\mathrm{ord}(g)$ S-potenzglatt, also

$$\mathrm{ord}(g) \mid \prod_i p^{\lfloor \log_{P_i}(S) \rfloor} .$$

Vorbemerkung

Sei $G = (G, +)$ eine endliche abelsche Gruppe, $g \in G$.

Es ist

$$\mathrm{ord}(g) \cdot g = O_G$$

Sei nun $\mathrm{ord}(g)$ S-potenzglatt, also

$$\mathrm{ord}(g) \mid \prod_i p^{\lfloor \log_{P_i}(S) \rfloor} .$$

Dann ist

$$\prod_i P_i^{\lfloor \log_{P_i}(S) \rfloor} \cdot g = O_G .$$

Faktorisierung

Sei $N = pq$.

Auch über dem Ring $\mathbf{Z}/(N)$ kann man elliptische Kurven betrachten.

Faktorisierung

Sei $N = pq$.

Auch über dem Ring $\mathbf{Z}/(N)$ kann man elliptische Kurven betrachten.

Für $E/(\mathbf{Z}/(N))$ haben wir die Gruppe $E(\mathbf{Z}/N\mathbf{Z})$.

Faktorisierung

Sei $N = pq$.

Auch über dem Ring $\mathbf{Z}/(N)$ kann man elliptische Kurven betrachten.

Für $E/(\mathbf{Z}/(N))$ haben wir die Gruppe $E(\mathbf{Z}/N\mathbf{Z})$.

Der Ringhomomorphismus

$$\mathbf{Z}/(N) \longrightarrow \mathbf{Z}/(p)$$

induziert dann einen Gruppenhomomorphismus

$$E(\mathbf{Z}/(N)) \longrightarrow E(\mathbf{Z}/(p)) \ , \ P \mapsto [P]_p$$

Faktorisierung

Sei $N = pq$.

Auch über dem Ring $\mathbf{Z}/(N)$ kann man elliptische Kurven betrachten.

Für $E/(\mathbf{Z}/(N))$ haben wir die Gruppe $E(\mathbf{Z}/N\mathbf{Z})$.

Der Ringhomomorphismus

$$\mathbf{Z}/(N) \longrightarrow \mathbf{Z}/(p)$$

induziert dann einen Gruppenhomomorphismus

$$E(\mathbf{Z}/(N)) \longrightarrow E(\mathbf{Z}/(p)) \ , \ P \mapsto [P]_p$$

Ebenso haben wir

$$E(\mathbf{Z}/(N)) \longrightarrow E(\mathbf{Z}/(q)) \ , \ P \mapsto [P]_q$$

Faktorisierung

Sei $N = pq$.

Auch über dem Ring $\mathbf{Z}/(N)$ kann man elliptische Kurven betrachten.

Für $E/(\mathbf{Z}/(N))$ haben wir die Gruppe $E(\mathbf{Z}/N\mathbf{Z})$.

Der Ringhomomorphismus

$$\mathbf{Z}/(N) \longrightarrow \mathbf{Z}/(p)$$

induziert dann einen Gruppenhomomorphismus

$$E(\mathbf{Z}/(N)) \longrightarrow E(\mathbf{Z}/(p)) \ , \ P \mapsto [P]_p$$

Ebenso haben wir

$$E(\mathbf{Z}/(N)) \longrightarrow E(\mathbf{Z}/(q)) \ , \ P \mapsto [P]_q \quad ,$$

Insgesamt einen Isomorphismus

$$E(\mathbf{Z}/(N)) \longrightarrow E(\mathbf{Z}/(p)) \times E(\mathbf{Z}/(q)) \ , \ P \mapsto ([P]_p, [P]_q).$$

Faktorisierung

Sei $E/(\mathbf{Z}/(N))$ eine elliptische Kurve, $P \in E(\mathbf{Z}/(N))$.

Angenommen nun: N hat Faktoren p, q (neben vielleicht weiteren) mit:

- $\mathrm{ord}([P]_p)$ ist S-potenzglatt
- $\mathrm{ord}([P]_q)$ ist nicht S-potenzglatt.

Faktorisierung

Sei $E/(\mathbf{Z}/(N))$ eine elliptische Kurve, $P \in E(\mathbf{Z}/(N))$.

Angenommen nun: N hat Faktoren p, q (neben vielleicht weiteren) mit:

- $\mathrm{ord}([P]_p)$ ist S-potenzglatt
- $\mathrm{ord}([P]_q)$ ist nicht S-potenzglatt.

Betrachte nun

$$Q := \prod_i P_i^{\lfloor \log_{P_i}(S) \rfloor} \cdot P \ .$$

Faktorisierung

Sei $E/(\mathbf{Z}/(N))$ eine elliptische Kurve, $P \in E(\mathbf{Z}/(N))$.

Angenommen nun: N hat Faktoren p, q (neben vielleicht weiteren) mit:

- $\mathrm{ord}([P]_p)$ ist S-potenzglatt
- $\mathrm{ord}([P]_q)$ ist nicht S-potenzglatt.

Betrachte nun

$$Q := \prod_i P_i^{\lfloor \log_{P_i}(S) \rfloor} \cdot P \ .$$

Es ist $[Q]_p = O, [Q]_q \neq O$.

Faktorisierung

Sei $E/(\mathbf{Z}/(N))$ eine elliptische Kurve, $P \in E(\mathbf{Z}/(N))$.

Angenommen nun: N hat Faktoren p, q (neben vielleicht weiteren) mit:

- $\mathrm{ord}([P]_p)$ ist S-potenzglatt
- $\mathrm{ord}([P]_q)$ ist nicht S-potenzglatt.

Betrachte nun

$$Q := \prod_i P_i^{\lfloor \log_{P_i}(S) \rfloor} \cdot P \ .$$

Es ist $[Q]_p = O, [Q]_q \neq O$.

Für $Q = (x(Q), y(Q))$: $\mathrm{ggT}(x(Q) - x(O), N)$ oder $\mathrm{ggT}(y(Q) - y(O), N)$ sind nicht-triviale Teiler von N.

Faktorisierung

Algorithmus.

Eingabe: N

1. Wähle eine Glattheitsschranke S und nummeriere die Primzahlen $\leq S$: $P_1, P_2, \ldots, P_k$.
2. Wähle eine elliptische Kurve E über $\mathbf{Z}/(N)$ und einen Punkt $P \in E(\mathbf{Z}/(N))$.
3. Berechne $Q := \prod_i P_i^{\lfloor \log_{P_i}(S) \rfloor} \cdot P$
4. Berechne die ggTs mit N wie oben.
5. Gegebenenfalls Faktoren ausgeben und / oder weitermachen.

Faktorisierung

Algorithmus.

Eingabe: N

1. Wähle eine Glattheitsschranke S und nummeriere die Primzahlen $\leq S$: $P_1, P_2, \ldots, P_k$.
2. Wähle eine elliptische Kurve E über $\mathbf{Z}/(N)$ und einen Punkt $P \in E(\mathbf{Z}/(N))$.
3. Berechne $Q := \prod_i P_i^{\lfloor \log_{P_i}(S) \rfloor} \cdot P \quad (\star)$
4. Berechne die ggTs mit N wie oben.
5. Gegebenenfalls Faktoren ausgeben und / oder weitermachen.

($\star$) mit "normalen Additionsformeln"; wenn Fehler, dann direkt zu 4.

Faktorisierung

Heuristische Laufzeitanalyse.

$$\exp((\sqrt{2} + o(1)) \cdot \sqrt{p \cdot \log(p)}\ ,$$

wobei p der kleinste Primteiler von N ist.

Heuristische Laufzeitanalyse.

$$\exp((\sqrt{2} + o(1)) \cdot \sqrt{p \cdot \log(p)}\,,$$

wobei p der kleinste Primteiler von N ist.

Also: Mit der Faktorisierung mit Elliptischen-Kurven kann man besonders schnell kleine Primteiler finden.

Hiermit kann man in den Faktorbasismethoden das Probeteilen vermeiden.