Discrete logarithm computation in finite fields $\mathbb{F}_{p^n}$ with the Number Field Sieve

Aurore Guillevic

Inria Nancy, Caramba team

June 11 & 13, 2019

Outline

Introduction

Index calculus algorithm

Coppersmith–Odlyzko–Schroeppel 1986
- Systematic relation collection: sieve
- Gaussian Integers $\mathbb{Z}[i]$
- Sieve with $\mathbb{Z}[i]$
- SageMath tests
- Recap

Factorization into prime ideals in quadratic number fields

Number Field Sieve with base-m

Number Field Sieve today: Joux–Lercier
- Rational reconstruction and lattice reduction
- Joux–Lercier polynomial selection method
- Example with monic f, g, principal K_f, K_g

Plan

Introduction

Index calculus algorithm

Coppersmith–Odlyzko–Schroeppel 1986

Factorization into prime ideals in quadratic number fields

Number Field Sieve with base-m

Number Field Sieve today: Joux–Lercier

Asymmetric cryptography

Factorization (RSA cryptosystem)

Discrete logarithm problem (use in Diffie-Hellman, etc)

Given a finite cyclic group $(\mathbf{G}, \cdot)$, a generator g and $h \in \mathbf{G}$, compute x s.t. $h = g^x$.

$\rightarrow$ can we invert the exponentiation function $(g, x) \mapsto g^x$?

Common choice of $\mathbf{G}$:

- prime finite field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ (1976)
- characteristic 2 field $\mathbb{F}_{2^n}$ ($\approx$ 1979)
- elliptic curve $E(\mathbb{F}_p)$ (1985)

Discrete log problem

How fast can we invert the exponentiation function $(g, x) \mapsto g^x$?

- $g \in \mathbf{G}$ generator, $\exists$ always a preimage $x \in \{1, \ldots, \#\mathbf{G}\}$
- naive search, try them all: $\#\mathbf{G}$ tests
- $O(\sqrt{\#G})$ algorithms
  - Shanks baby-step-giant-step (BSGS): $O(\sqrt{\#\mathbf{G}})$, deterministic
  - random walk in $\mathbf{G}$, cycle path finding algorithm in a connected graph (Floyd) $\rightarrow$ Pollard: $O(\sqrt{\#\mathbf{G}})$, probabilistic (the cycle path encodes the answer)
  - parallel search (parallel Pollard, Kangarous)
- independent search in each distinct subgroup + CRT (Pohlig-Hellman)

Discrete log problem

How fast can we invert the exponentiation function $(g, x) \mapsto g^x$?

- $g \in \mathbf{G}$ generator, $\exists$ always a preimage $x \in \{1, \ldots, \#\mathbf{G}\}$
- naive search, try them all: $\#\mathbf{G}$ tests
- $O(\sqrt{\#G})$ algorithms
  - Shanks baby-step-giant-step (BSGS): $O(\sqrt{\#\mathbf{G}})$, deterministic
  - random walk in $\mathbf{G}$, cycle path finding algorithm in a connected graph (Floyd) $\rightarrow$ Pollard: $O(\sqrt{\#\mathbf{G}})$, probabilistic (the cycle path encodes the answer)
  - parallel search (parallel Pollard, Kangarous)
- independent search in each distinct subgroup + CRT (Pohlig-Hellman)

$\rightarrow$ Choose $\mathbf{G}$ of large prime order (no subgroup)

$\rightarrow$ complexity of inverting exponentiation in $O(\sqrt{\#G})$

$\rightarrow$ security level 128 bits means $\sqrt{\#G} \geq 2^{128} \rightarrow \#G \geq 2^{256}$
analogy with symmetric crypto, keylength 128 bits (16 bytes)

Discrete log problem

How fast can we invert the exponentiation function $(g, x) \mapsto g^x$?

G cyclic group of prime order, complexity $O(\sqrt{\#G})$.

Discrete log problem

How fast can we invert the exponentiation function $(g, x) \mapsto g^x$?

G cyclic group of prime order, complexity $O(\sqrt{\#G})$.

better way?

Discrete log problem

How fast can we invert the exponentiation function $(g, x) \mapsto g^x$?

G cyclic group of prime order, complexity $O(\sqrt{\#G})$.

better way?
$\rightarrow$ Use additional structure of **G** if any.

Plan

Introduction

Index calculus algorithm

Coppersmith–Odlyzko–Schroeppel 1986

Factorization into prime ideals in quadratic number fields

Number Field Sieve with base-m

Number Field Sieve today: Joux–Lercier

Discrete log problem when $\mathbf{G} = (\mathbb{Z}/p\mathbb{Z})^*$

Index calculus algorithm [Western–Miller 68, Adleman 79], prequel of the Number Field Sieve algorithm (NFS)

- p prime, $(p-1)/4$ prime, $\mathbf{G} = (\mathbb{Z}/p\mathbb{Z})^*$, gen. g, target h
- get many multiplicative relations in $\mathbf{G}$
  $g^t = g_1^{e_1} g_2^{e_2} \cdots g_i^{e_i} \pmod p$, $g, g_1, g_2, \ldots, g_i \in \mathbf{G}$
- find a relation $h = g_1^{e_1'} g_2^{e_2'} \cdots g_i^{e_i'} \pmod p$
- take logarithm: linear relations

$$\begin{aligned} t &= e_1 \log_g g_1 + e_2 \log_g g_2 + \ldots + e_i \log_g g_i \pmod{p-1} \\ &\vdots \\ \log_g h &= e_1' \log_g g_1 + e_2' \log_g g_2 + \ldots + e_i' \log_g g_i \pmod{p-1} \end{aligned}$$

- solve a linear system
- get $x = \log_g h$

Index calculus in $(\mathbb{Z}/p\mathbb{Z})^*$: example

`example-1109-index-calculus.sage`

$p = 1109$, $r = (p-1)/4 = 277$ prime

Smoothness bound $B = 13$

$\mathcal{F}_{13} = \{2, 3, 5, 7, 11, 13\}$ small primes up to B, $i = \#\mathcal{F}$

B-smooth integer: $n = \prod_{p_i \leq B} p_i^{e_i}$, p_i prime

is $g^s \bmod p = n$ smooth? $1 \leq s \leq 72$ is enough

$$\begin{aligned} g^{1} &= 2 = 2 \\ g^{13} &= 429 = 3 \cdot 11 \cdot 13 \\ g^{16} &= 105 = 3 \cdot 5 \cdot 7 \\ g^{21} &= 33 = 3 \cdot 11 \\ g^{44} &= 1029 = 3 \cdot 7^3 \\ g^{72} &= 325 = 5^2 \cdot 13 \end{aligned} \quad \rightarrow \quad \begin{matrix} 2 & 3 & 5 & 7 & 11 & 13 \end{matrix} \; \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 3 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 1 \end{bmatrix} \cdot \boldsymbol{x} = \begin{bmatrix} 1 \\ 13 \\ 16 \\ 21 \\ 44 \\ 72 \end{bmatrix}$$

$\boldsymbol{x} = [1, 219, 40, 34, 79, 269] \bmod 277$

$\rightarrow \log_g 7 = 34 \bmod 277$, that is, $(g^{34})^4 = 7^4$

$g^{34} = 7u$ and $u^4 = 1$

Index calculus in $(\mathbb{Z}/p\mathbb{Z})^*$: example

$\boldsymbol{x} = [1, 219, 40, 34, 79, 269] \bmod 277$

subgroup of order 4: $g_4 = g^{(p-1)/4}$

$\{1, g_4, g_4^2, g_4^3\} = \{1, 354, 1108, 755\}$

Pohlig-Hellman:

$$\begin{aligned}
3/g^{219} &= \quad = \quad 1 \Rightarrow \log_g 3 = && = 219 \\
5/g^{40} &= 1108 = -1 \Rightarrow \log_g 5 = 40 + (p-1)/2 && = 594 \\
7/g^{34} &= 354 = g_4 \Rightarrow \log_g 7 = 34 + (p-1)/4 && = 311 \\
11/g^{79} &= 755 = g_4^3 \Rightarrow \log_g 11 = 79 + 3(p-1)/4 && = 910 \\
13/g^{269} &= 755 = g_4^3 \Rightarrow \log_g 13 = 269 + 3(p-1)/4 && = 1100
\end{aligned}$$

$\boldsymbol{v} = [1, 219, 594, 311, 910, 1100] \bmod p-1$

Target $h = 777$

$g^{10} \cdot 777 = 495 = 3^2 \cdot 5 \cdot 11 \bmod p$

$\log_2 777 = -10 + 2\log_g 3 + \log_g 5 + \log_g 11 = 824 \bmod p-1$

$g^{824} = 777$

Index calculus in $(\mathbb{Z}/p\mathbb{Z})^*$

Trick

Multiplicative relations over the **integers**

$g_1, g_2, \ldots, g_i \longleftrightarrow$ small prime integers

Smooth integers $n = \prod_{p_i \leq B} p_i^{e_i}$ are quite common $\rightarrow$ it works

Complexity $e^{\sqrt{(2+o(1))(\log p)(\log \log p)}}$ (Pomerance 87)

Index calculus in $(\mathbb{Z}/p\mathbb{Z})^*$

Trick

Multiplicative relations over the **integers**

$g_1, g_2, \ldots, g_i \longleftrightarrow$ small prime integers

Smooth integers $n = \prod_{p_i \leq B} p_i^{e_i}$ are quite common $\rightarrow$ it works

Complexity $e^{\sqrt{(2+o(1))(\log p)(\log\log p)}}$ (Pomerance 87)

Improvements in the 80's, 90's:

- Sieve (faster relation collection)
- Smaller integers to factor
- Multiplicative relations in **number fields**
- Better **sparse linear algebra**
- Independent targets h

Plan

Introduction

Index calculus algorithm

Coppersmith–Odlyzko–Schroeppel 1986

- Systematic relation collection: sieve
- Gaussian Integers $\mathbb{Z}[i]$
- Sieve with $\mathbb{Z}[i]$
- SageMath tests
- Recap

Factorization into prime ideals in quadratic number fields

Number Field Sieve with base-m

Number Field Sieve today: Joux–Lercier

Sieve: Coppersmith–Odlyzko–Schroeppel 1986

$H = \lceil \sqrt{p} \rceil$, $J = H^2 - p$, $|J - 1/4| < \sqrt{p}$

- small integers a, b in $[-A, A]$
  $A = e^{(1/2+\varepsilon)\sqrt{\log p \log\log p}}$

$$(H+a)(H+b) \equiv n = \underbrace{(H^2 - p)}_{J \approx \sqrt{p}} + (a+b)H + ab \bmod p$$

- Collect smooth

$$\underbrace{(H+a)(H+b)}_{\text{do not factor further}} \equiv n = \underbrace{J}_{\sqrt{p}} + \underbrace{(a+b)H}_{2A\sqrt{p}} + \underbrace{ab}_{A^2} = \prod_{p_i < B} p_i^{e_i}$$

- If n is B-smooth, store the relation

$$\log(H+a) + \log(H+b) = \sum_{p_i < B} e_i \log p_i \mod p-1$$

Quadratic Sieve in $(\mathbb{Z}/p\mathbb{Z})^*$: example $p = 1109$

example-1109-COS-sieve-L.sage

Prime $p = 1109$, prime $r = (p-1)/4 = 277$
$H = \lceil \sqrt{p} \rfloor = 33$ ($\sqrt{p} = 33.301$)
$J = H^2 - p = -20$
$L = L[1/2] = e^{1/2\sqrt{\log p \log\log p}} = 6.345$
Smoothness bound $B = 11$
Factor basis $\mathcal{F}_{\text{low}} = \{2, 3, 5, 7, 11\}$
Sieving bound $A = 5$ ($a, b \in [-5, 5]$)
Factor basis $\mathcal{F}_{\text{high}} = \{H - A, \ldots, H + A\} = \{28, \ldots, 38\}$

16 relations needed
Sieving space $\#\{(a, b)\} = A'(A'+1)/2 = 66$ where $A' = 2A + 1$

Quadratic Sieve in $(\mathbb{Z}/p\mathbb{Z})^*$: example $p = 1109$

a, b	$(H+a)\cdot(H+b)$	n=factor(n)
$-5, -4$	$28\cdot29$	$-297 = -3^3 \cdot 11$
$-5, 5$	$28\cdot38$	$-45 = -3^2 \cdot 5$
$-4, -2$	$29\cdot31$	$-210 = -2 \cdot 3 \cdot 5 \cdot 7$
$-4, 4$	$29\cdot37$	$-36 = -2^2 \cdot 3^2$
$-4, 5$	$29\cdot38$	$-7 = -7$
$-3, 4$	$30\cdot37$	$1 = 1$
$-2, 1$	$31\cdot34$	$-55 = -5 \cdot 11$
$-2, 2$	$31\cdot35$	$-24 = -2^3 \cdot 3$
$-2, 3$	$31\cdot36$	$7 = 7$
$-1, 1$	$32\cdot34$	$-21 = -3 \cdot 7$
$-1, 2$	$32\cdot35$	$11 = 11$
$-1, 4$	$32\cdot37$	$75 = 3 \cdot 5^2$
$0, 0$	$33\cdot33$	$-20 = -2^2 \cdot 5$
$0, 4$	$33\cdot37$	$112 = 2^4 \cdot 7$
$1, 2$	$34\cdot35$	$81 = 3^4$
$4, 5$	$37\cdot38$	$297 = 3^3 \cdot 11$

Quadratic Sieve in $(\mathbb{Z}/p\mathbb{Z})^*$: example $p = 1109$

$$
\begin{array}{cccccccccccccccc}
2 & 3 & 5 & 7 & 11 & 28 & 29 & 30 & 31 & 32 & 33 & 34 & 35 & 36 & 37 & 38
\end{array}
$$

$$
\begin{bmatrix}
0 & 3 & 0 & 0 & 1 & -1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 2 & 1 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \\
1 & 1 & 1 & 1 & 0 & 0 & -1 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
2 & 2 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 \\
0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & -1 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \\
3 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\
0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & -1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & -1 & 0 & 0 & 0 \\
0 & 1 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & -1 & 0 \\
2 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -2 & 0 & 0 & 0 & 0 & 0 \\
4 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & -1 & 0 \\
0 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & -1 & 0 & 0 & 0 \\
0 & 3 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & -1
\end{bmatrix}
$$

Quadratic Sieve in $(\mathbb{Z}/p\mathbb{Z})^*$: example $p = 1109$

2	3	5	7	11	28	29	30	31	32	33	34	35	36	37	38
0	3			1	−1	−1									
	2	1			−1										−1
1	1	1	1			−1		−1							
2	2					−1								−1	
			1			−1									−1
							−1							−1	
		1		1				−1			−1				
3	1							−1				−1			
			1					−1					−1		
	1		1						−1		−1				
				1					−1			−1			
	1	2							−1					−1	
2		1								−2					
4			1							−1				−1	
	4										−1	−1			
	3			1										−1	−1

Quadratic Sieve in $(\mathbb{Z}/p\mathbb{Z})^*$: example $p = 1109$

Right kernel $M \cdot \boldsymbol{x} = 0 \bmod (p-1)/4 = 277$:

$$\boldsymbol{x} = (\underbrace{1, 219, 40, 34, 79}_{\mathcal{F}_{\text{low}}}, \underbrace{36, 146, 260, 148, 5, 21, 248, 74, 163, 17, 165}_{\mathcal{F}_{\text{high}}})$$

Logarithms in basis $g_0 = 2$ since $x_0 = 1 = \log 2$

$\rightarrow$ order 4 subgroup

$\boldsymbol{v} =$
$[\mathbf{1}, \mathbf{219}, \mathbf{594}, \mathbf{311}, \mathbf{910}, 313, 700, 814, 979, 5, 21, 1079, 905, 440, 294, 165]$
$\bmod p - 1$

Quadratic Sieve in $(\mathbb{Z}/p\mathbb{Z})^*$: example $p = 1109$

Right kernel $M \cdot \boldsymbol{x} = 0 \bmod (p-1)/4 = 277$:

$$\boldsymbol{x} = (\underbrace{1, 219, 40, 34, 79}_{\mathcal{F}_{\text{low}}}, \underbrace{36, 146, 260, 148, 5, 21, 248, 74, 163, 17, 165}_{\mathcal{F}_{\text{high}}})$$

Logarithms in basis $g_0 = 2$ since $x_0 = 1 = \log 2$

$\rightarrow$ order 4 subgroup

$\boldsymbol{v} = [\mathbf{1}, \mathbf{219}, \mathbf{594}, \mathbf{311}, \mathbf{910}, 313, 700, 814, 979, 5, 21, 1079, 905, 440, 294, 165] \bmod p - 1$

Previously found:

$\boldsymbol{v} = [1, 219, 594, 311, 910, 1100] \bmod p - 1$

Sieve: Coppersmith–Odlyzko–Schroeppel 1986

Sieve: faster smoothness tests

Erathostene sieve: remaining numbers are prime
COS sieve: remaining numbers are not smooth: discard them

1. initialize a tabular T of norms, indexed by a, b
2. sieve for q in $2, 2^2, 2^3, 2^4, 3, 3^2, 3^3, 5, 5^2, 7, 11$
3. the cells $T[i][j] \in \{-1, 1\}$ give relations for $(a, b) = (i - A, j - A)$

Numerical example follows.

Sieve: Coppersmith–Odlyzko–Schroeppel 1986

	−5	−4	−3	−2	−1	0	1	2	3	4	5
−5	−325	−297	−269	−241	−213	−185	−157	−129	−101	−73	−45
−4	−297	−268	−239	−210	−181	−152	−123	−94	−65	−36	−7
−3	−269	−239	−209	−179	−149	−119	−89	−59	−29	1	31
−2	−241	−210	−179	−148	−117	−86	−55	−24	7	38	69
−1	−213	−181	−149	−117	−85	−53	−21	11	43	75	107
0	−185	−152	−119	−86	−53	−20	13	46	79	112	145
1	−157	−123	−89	−55	−21	13	47	81	115	149	183
2	−129	−94	−59	−24	11	46	81	116	151	186	221
3	−101	−65	−29	7	43	79	115	151	187	223	259
4	−73	−36	1	38	75	112	149	186	223	260	297
5	−45	−7	31	69	107	145	183	221	259	297	335

Sieve: Coppersmith–Odlyzko–Schroeppel 1986

	−5	−4	−3	−2	−1	0	1	2	3	4	5
−5	−325	−297	−269	−241	−213	−185	−157	−129	−101	−73	−45
−4		−268	−239	−210	−181	−152	−123	−94	−65	−36	−7
−3			−209	−179	−149	−119	−89	−59	−29	1	31
−2				−148	−117	−86	−55	−24	7	38	69
−1					−85	−53	−21	11	43	75	107
0						−20	13	46	79	112	145
1							47	81	115	149	183
2								116	151	186	221
3									187	223	259
4										260	297
5											335

a, b have symmetric roles: $a \leq b$

Sieve: Coppersmith–Odlyzko–Schroeppel 1986

	−5	−4	−3	−2	−1	0	1	2	3	4	5
−5	−325	−297	−269	−241	−213	−185	−157	−129	−101	−73	−45
−4		−268	−239	−210	−181	−152	−123	−94	−65	−36	−7
−3			−209	−179	−149	−119	−89	−59	−29	1	31
−2				−148	−117	−86	−55	−24	7	38	69
−1					−85	−53	−21	11	43	75	107
0						−20	13	46	79	112	145
1							47	81	115	149	183
2								116	151	186	221
3									187	223	259
4										260	297
5											335

$q = 2$

Sieve: Coppersmith–Odlyzko–Schroeppel 1986

	−5	−4	−3	−2	−1	0	1	2	3	4	5
−5	−325	−297	−269	−241	−213	−185	−157	−129	−101	−73	−45
−4		−134	−239	−105	−181	−76	−123	−47	−65	−18	−7
−3			−209	−179	−149	−119	−89	−59	−29	1	31
−2				−74	−117	−43	−55	−12	7	19	69
−1					−85	−53	−21	11	43	75	107
0						−10	13	23	79	56	145
1							47	81	115	149	183
2								58	151	93	221
3									187	223	259
4										130	297
5											335

$q = 2$

Sieve: Coppersmith–Odlyzko–Schroeppel 1986

	−5	−4	−3	−2	−1	0	1	2	3	4	5
−5	−325	−297	−269	−241	−213	−185	−157	−129	−101	−73	−45
−4		−134	−239	−105	−181	−76	−123	−47	−65	−18	−7
−3			−209	−179	−149	−119	−89	−59	−29	1	31
−2				−74	−117	−43	−55	−12	7	19	69
−1					−85	−53	−21	11	43	75	107
0						−10	13	23	79	56	145
1							47	81	115	149	183
2								58	151	93	221
3									187	223	259
4										130	297
5											335

$q = 2^2$

Sieve: Coppersmith–Odlyzko–Schroeppel 1986

	−5	−4	−3	−2	−1	0	1	2	3	4	5
−5	−325	−297	−269	−241	−213	−185	−157	−129	−101	−73	−45
−4		−67	−239	−105	−181	−38	−123	−47	−65	−9	−7
−3			−209	−179	−149	−119	−89	−59	−29	1	31
−2				−37	−117	−43	−55	−6	7	19	69
−1					−85	−53	−21	11	43	75	107
0						−5	13	23	79	28	145
1							47	81	115	149	183
2								29	151	93	221
3									187	223	259
4										65	297
5											335

$q = 2^2$

Sieve: Coppersmith–Odlyzko–Schroeppel 1986

	−5	−4	−3	−2	−1	0	1	2	3	4	5
−5	−325	−297	−269	−241	−213	−185	−157	−129	−101	−73	−45
−4		−67	−239	−105	−181	−38	−123	−47	−65	−9	−7
−3			−209	−179	−149	−119	−89	−59	−29	1	31
−2				−37	−117	−43	−55	−6	7	19	69
−1					−85	−53	−21	11	43	75	107
0						−5	13	23	79	28	145
1							47	81	115	149	183
2								29	151	93	221
3									187	223	259
4										65	297
5											335

$q = 2^3$

Sieve: Coppersmith–Odlyzko–Schroeppel 1986

	−5	−4	−3	−2	−1	0	1	2	3	4	5
−5	−325	−297	−269	−241	−213	−185	−157	−129	−101	−73	−45
−4		−67	−239	−105	−181	−19	−123	−47	−65	−9	−7
−3			−209	−179	−149	−119	−89	−59	−29	1	31
−2				−37	−117	−43	−55	−3	7	19	69
−1					−85	−53	−21	11	43	75	107
0						−5	13	23	79	14	145
1							47	81	115	149	183
2								29	151	93	221
3									187	223	259
4										65	297
5											335

$q = 2^3$

Sieve: Coppersmith–Odlyzko–Schroeppel 1986

	−5	−4	−3	−2	−1	0	1	2	3	4	5
−5	−325	−297	−269	−241	−213	−185	−157	−129	−101	−73	−45
−4		−67	−239	−105	−181	−19	−123	−47	−65	−9	−7
−3			−209	−179	−149	−119	−89	−59	−29	1	31
−2				−37	−117	−43	−55	−3	7	19	69
−1					−85	−53	−21	11	43	75	107
0						−5	13	23	79	14	145
1							47	81	115	149	183
2								29	151	93	221
3									187	223	259
4										65	297
5											335

$q = 2^4$

Sieve: Coppersmith–Odlyzko–Schroeppel 1986

	−5	−4	−3	−2	−1	0	1	2	3	4	5
−5	−325	−297	−269	−241	−213	−185	−157	−129	−101	−73	−45
−4		−67	−239	−105	−181	−19	−123	−47	−65	−9	−7
−3			−209	−179	−149	−119	−89	−59	−29	1	31
−2				−37	−117	−43	−55	−3	7	19	69
−1					−85	−53	−21	11	43	75	107
0						−5	13	23	79	7	145
1							47	81	115	149	183
2								29	151	93	221
3									187	223	259
4										65	297
5											335

$q = 2^4$

Sieve: Coppersmith–Odlyzko–Schroeppel 1986

	−5	−4	−3	−2	−1	0	1	2	3	4	5
−5	−325	−297	−269	−241	−213	−185	−157	−129	−101	−73	−45
−4		−67	−239	−105	−181	−19	−123	−47	−65	−9	−7
−3			−209	−179	−149	−119	−89	−59	−29	1	31
−2				−37	−117	−43	−55	−3	7	19	69
−1					−85	−53	−21	11	43	75	107
0						−5	13	23	79	7	145
1							47	81	115	149	183
2								29	151	93	221
3									187	223	259
4										65	297
5											335

$q = 3$

Sieve: Coppersmith–Odlyzko–Schroeppel 1986

	−5	−4	−3	−2	−1	0	1	2	3	4	5
−5	−325	−99	−269	−241	−71	−185	−157	−43	−101	−73	−15
−4		−67	−239	−35	−181	−19	−41	−47	−65	−3	−7
−3			−209	−179	−149	−119	−89	−59	−29	1	31
−2				−37	−39	−43	−55	−1	7	19	23
−1					−85	−53	−7	11	43	25	107
0						−5	13	23	79	7	145
1							47	27	115	149	61
2								29	151	31	221
3									187	223	259
4										65	99
5											335

$q = 3$

Sieve: Coppersmith–Odlyzko–Schroeppel 1986

	−5	−4	−3	−2	−1	0	1	2	3	4	5
−5	−325	−99	−269	−241	−71	−185	−157	−43	−101	−73	−15
−4		−67	−239	−35	−181	−19	−41	−47	−65	−3	−7
−3			−209	−179	−149	−119	−89	−59	−29	1	31
−2				−37	−39	−43	−55	−1	7	19	23
−1					−85	−53	−7	11	43	25	107
0						−5	13	23	79	7	145
1							47	27	115	149	61
2								29	151	31	221
3									187	223	259
4										65	99
5											335

$q = 3^2$

Sieve: Coppersmith–Odlyzko–Schroeppel 1986

	−5	−4	−3	−2	−1	0	1	2	3	4	5
−5	−325	−33	−269	−241	−71	−185	−157	−43	−101	−73	−5
−4		−67	−239	−35	−181	−19	−41	−47	−65	−1	−7
−3			−209	−179	−149	−119	−89	−59	−29	1	31
−2				−37	−13	−43	−55	−1	7	19	23
−1					−85	−53	−7	11	43	25	107
0						−5	13	23	79	7	145
1							47	9	115	149	61
2								29	151	31	221
3									187	223	259
4										65	33
5											335

$q = 3^2$

Sieve: Coppersmith–Odlyzko–Schroeppel 1986

	−5	−4	−3	−2	−1	0	1	2	3	4	5
−5	−325	−33	−269	−241	−71	−185	−157	−43	−101	−73	−5
−4		−67	−239	−35	−181	−19	−41	−47	−65	−1	−7
−3			−209	−179	−149	−119	−89	−59	−29	1	31
−2				−37	−13	−43	−55	−1	7	19	23
−1					−85	−53	−7	11	43	25	107
0						−5	13	23	79	7	145
1							47	9	115	149	61
2								29	151	31	221
3									187	223	259
4										65	33
5											335

$q = 3^3$

Sieve: Coppersmith–Odlyzko–Schroeppel 1986

	−5	−4	−3	−2	−1	0	1	2	3	4	5
−5	−325	−11	−269	−241	−71	−185	−157	−43	−101	−73	−5
−4		−67	−239	−35	−181	−19	−41	−47	−65	−1	−7
−3			−209	−179	−149	−119	−89	−59	−29	1	31
−2				−37	−13	−43	−55	−1	7	19	23
−1					−85	−53	−7	11	43	25	107
0						−5	13	23	79	7	145
1							47	3	115	149	61
2								29	151	31	221
3									187	223	259
4										65	11
5											335

$q = 3^3$

Sieve: Coppersmith–Odlyzko–Schroeppel 1986

	−5	−4	−3	−2	−1	0	1	2	3	4	5
−5	−325	−11	−269	−241	−71	−185	−157	−43	−101	−73	−5
−4		−67	−239	−35	−181	−19	−41	−47	−65	−1	−7
−3			−209	−179	−149	−119	−89	−59	−29	1	31
−2				−37	−13	−43	−55	−1	7	19	23
−1					−85	−53	−7	11	43	25	107
0						−5	13	23	79	7	145
1							47	3	115	149	61
2								29	151	31	221
3									187	223	259
4										65	11
5											335

$q = 3^4$

Sieve: Coppersmith–Odlyzko–Schroeppel 1986

	−5	−4	−3	−2	−1	0	1	2	3	4	5
−5	−325	−11	−269	−241	−71	−185	−157	−43	−101	−73	−5
−4		−67	−239	−35	−181	−19	−41	−47	−65	−1	−7
−3			−209	−179	−149	−119	−89	−59	−29	1	31
−2				−37	−13	−43	−55	−1	7	19	23
−1					−85	−53	−7	11	43	25	107
0						−5	13	23	79	7	145
1							47	1	115	149	61
2								29	151	31	221
3									187	223	259
4										65	11
5											335

$q = 3^4$

Sieve: Coppersmith–Odlyzko–Schroeppel 1986

	−5	−4	−3	−2	−1	0	1	2	3	4	5
−5	−325	−11	−269	−241	−71	−185	−157	−43	−101	−73	−5
−4		−67	−239	−35	−181	−19	−41	−47	−65	−1	−7
−3			−209	−179	−149	−119	−89	−59	−29	1	31
−2				−37	−13	−43	−55	−1	7	19	23
−1					−85	−53	−7	11	43	25	107
0						−5	13	23	79	7	145
1							47	1	115	149	61
2								29	151	31	221
3									187	223	259
4										65	11
5											335

$q = 5$

Sieve: Coppersmith–Odlyzko–Schroeppel 1986

	−5	−4	−3	−2	−1	0	1	2	3	4	5
−5	−65	−11	−269	−241	−71	−37	−157	−43	−101	−73	−1
−4		−67	−239	−7	−181	−19	−41	−47	−13	−1	−7
−3			−209	−179	−149	−119	−89	−59	−29	1	31
−2				−37	−13	−43	−11	−1	7	19	23
−1					−17	−53	−7	11	43	5	107
0						−1	13	23	79	7	29
1							47	1	23	149	61
2								29	151	31	221
3									187	223	259
4										13	11
5											67

$q = 5$

Sieve: Coppersmith–Odlyzko–Schroeppel 1986

	−5	−4	−3	−2	−1	0	1	2	3	4	5
−5	−65	−11	−269	−241	−71	−37	−157	−43	−101	−73	−1
−4		−67	−239	−7	−181	−19	−41	−47	−13	−1	−7
−3			−209	−179	−149	−119	−89	−59	−29	1	31
−2				−37	−13	−43	−11	−1	7	19	23
−1					−17	−53	−7	11	43	5	107
0						−1	13	23	79	7	29
1							47	1	23	149	61
2								29	151	31	221
3									187	223	259
4										13	11
5											67

$q = 5^2$

Sieve: Coppersmith–Odlyzko–Schroeppel 1986

	−5	−4	−3	−2	−1	0	1	2	3	4	5
−5	−13	−11	−269	−241	−71	−37	−157	−43	−101	−73	−1
−4		−67	−239	−7	−181	−19	−41	−47	−13	−1	−7
−3			−209	−179	−149	−119	−89	−59	−29	1	31
−2				−37	−13	−43	−11	−1	7	19	23
−1					−17	−53	−7	11	43	1	107
0						−1	13	23	79	7	29
1							47	1	23	149	61
2								29	151	31	221
3									187	223	259
4										13	11
5											67

$q = 5^2$

Sieve: Coppersmith–Odlyzko–Schroeppel 1986

	−5	−4	−3	−2	−1	0	1	2	3	4	5
−5	−13	−11	−269	−241	−71	−37	−157	−43	−101	−73	−1
−4		−67	−239	−7	−181	−19	−41	−47	−13	−1	−7
−3			−209	−179	−149	−119	−89	−59	−29	1	31
−2				−37	−13	−43	−11	−1	7	19	23
−1					−17	−53	−7	11	43	1	107
0						−1	13	23	79	7	29
1							47	1	23	149	61
2								29	151	31	221
3									187	223	259
4										13	11
5											67

$q = 7$

Sieve: Coppersmith–Odlyzko–Schroeppel 1986

	−5	−4	−3	−2	−1	0	1	2	3	4	5
−5	−13	−11	−269	−241	−71	−37	−157	−43	−101	−73	−1
−4		−67	−239	−1	−181	−19	−41	−47	−13	−1	−1
−3			−209	−179	−149	−17	−89	−59	−29	1	31
−2				−37	−13	−43	−11	−1	1	19	23
−1					−17	−53	−1	11	43	1	107
0						−1	13	23	79	1	29
1							47	1	23	149	61
2								29	151	31	221
3									187	223	37
4										13	11
5											67

$q = 7$

Sieve: Coppersmith–Odlyzko–Schroeppel 1986

	−5	−4	−3	−2	−1	0	1	2	3	4	5
−5	−13	−11	−269	−241	−71	−37	−157	−43	−101	−73	−1
−4		−67	−239	−1	−181	−19	−41	−47	−13	−1	−1
−3			−209	−179	−149	−17	−89	−59	−29	1	31
−2				−37	−13	−43	−11	−1	1	19	23
−1					−17	−53	−1	11	43	1	107
0						−1	13	23	79	1	29
1							47	1	23	149	61
2								29	151	31	221
3									187	223	37
4										13	11
5											67

$q = 11$

Sieve: Coppersmith–Odlyzko–Schroeppel 1986

	−5	−4	−3	−2	−1	0	1	2	3	4	5
−5	−13	−1	−269	−241	−71	−37	−157	−43	−101	−73	−1
−4		−67	−239	−1	−181	−19	−41	−47	−13	−1	−1
−3			−19	−179	−149	−17	−89	−59	−29	1	31
−2				−37	−13	−43	−1	−1	1	19	23
−1					−17	−53	−1	1	43	1	107
0						−1	13	23	79	1	29
1							47	1	23	149	61
2								29	151	31	221
3									17	223	37
4										13	1
5											67

$q = 11$

Sieve: Coppersmith–Odlyzko–Schroeppel 1986

	−5	−4	−3	−2	−1	0	1	2	3	4	5
−5	−13	−1	−269	−241	−71	−37	−157	−43	−101	−73	−1
−4		−67	−239	−1	−181	−19	−41	−47	−13	−1	−1
−3			−19	−179	−149	−17	−89	−59	−29	1	31
−2				−37	−13	−43	−1	−1	1	19	23
−1					−17	−53	−1	1	43	1	107
0						−1	13	23	79	1	29
1							47	1	23	149	61
2								29	151	31	221
3									17	223	37
4										13	1
5											67

$B = 11$

Sieve: Coppersmith–Odlyzko–Schroeppel 1986

	-5	-4	-3	-2	-1	0	1	2	3	4	5
-5		-1									-1
-4				-1						-1	-1
-3										1	
-2							-1	-1	1		
-1							-1	1		1	
0						-1				1	
1								1			
2											
3											
4											1
5											

$B = 11$

Sieve: Coppersmith–Odlyzko–Schroeppel 1986

a, b	$(H + a)\cdot(H + b)$	n=factor(n)
$-5, -4$	$28\cdot29$	$-297 = -3^3 \cdot 11$
$-5, 5$	$28\cdot38$	$-45 = -3^2 \cdot 5$
$-4, -2$	$29\cdot31$	$-210 = -2 \cdot 3 \cdot 5 \cdot 7$
$-4, 4$	$29\cdot37$	$-36 = -2^2 \cdot 3^2$
$-4, 5$	$29\cdot38$	$-7 = -7$
$-3, 4$	$30\cdot37$	$1 = 1$
$-2, 1$	$31\cdot34$	$-55 = -5 \cdot 11$
$-2, 2$	$31\cdot35$	$-24 = -2^3 \cdot 3$
$-2, 3$	$31\cdot36$	$7 = 7$
$-1, 1$	$32\cdot34$	$-21 = -3 \cdot 7$
$-1, 2$	$32\cdot35$	$11 = 11$
$-1, 4$	$32\cdot37$	$75 = 3 \cdot 5^2$
$0, 0$	$33\cdot33$	$-20 = -2^2 \cdot 5$
$0, 4$	$33\cdot37$	$112 = 2^4 \cdot 7$
$1, 2$	$34\cdot35$	$81 = 3^4$
$4, 5$	$37\cdot38$	$297 = 3^3 \cdot 11$

Gaussian Integers $\mathbb{Z}[i]$ for DL in $\mathrm{GF}(p^2)$

Meanwhile,
1985: ElGamal designed an algorithm to compute DLs in $\mathrm{GF}(p^2)$ with two quadratic number fields

1986: Coppersmith, Odlyzko, and Schroeppel applied it to $\mathrm{GF}(p)$

Coppersmith–Odlyzko–Schroeppel 1986: $\mathbb{Z}[i]$

reduce further the size of the integers to factor

If $p = 1 \bmod 4$, $\exists\ U, V$ s.t. $p = U^2 + V^2$
and $|U|, |V| < \sqrt{p}$
$U/V \equiv m \mod p$ and $m^2 + 1 = 0 \mod p$

Define a map from $\mathbb{Z}[i]$ to $\mathbb{Z}/p\mathbb{Z}$

$$\begin{aligned} \phi\colon \mathbb{Z}[i] &\to \mathbb{Z}/p\mathbb{Z} \\ i &\mapsto m \bmod p \text{ where } m = U/V,\ m^2+1 = 0 \bmod p \end{aligned}$$

ring homomorphism $\phi(a + bi) = a + bm$

$$\phi(\underbrace{a + bi}_{\substack{\text{factor in} \\ \mathbb{Z}[i]}}) = a + bm = (a + b\ \underbrace{U/V}_{=m}) = (\underbrace{aV + bU}_{\text{factor in } \mathbb{Z}})V^{-1} \mod p$$

Example in $\mathbb{Z}[i]$

$p = 1109 = 1 \bmod 4,\ r = (p-1)/4 = 277$ prime
$p = 22^2 + 25^2$
$\max(|a|, |b|) = A = 20,\ B = 13$ smoothness bound

Rational side

$\mathcal{F}_{\text{rat}} = \{2, 3, 5, 7, 11, 13\}$ primes up to B

Algebraic side: think about the complex number in $\mathbb{C}$

$(1+i)(1-i) = 2,\ (2+i)(2-i) = 5,\ (2+3i)(2-3i) = 13$
All primes $p = 1 \bmod 4$

- can be written as a sum of two squares $p = a^2 + b^2$
- factor into two conjugate Gaussian integers $(a+ib)(a-ib)$

Units: $i^2 = -1$

$\mathcal{F}_{\text{alg}} = \{1+i, 1-i, 2+i, 2-i, 2+3i, 2-3i\}$
"primes" of norm up to B
$\mathcal{U}_{\text{alg}} = \{-1, i, -i\}$ Units

Example in $\mathbb{Z}[i]$

$p = 1109$

$(a, b) = (-4, 7)$,
$\text{Norm}(-4 + 7i) = (-4)^2 + 7^2 = 65 = 5 \cdot 13$

In $\mathbb{Z}[i]$,

- $5 = (2 + i)(2 - i)$
- $13 = (2 + 3i)(2 - 3i)$

Then,

- → each of $(2 \pm i)(2 \pm 3i)$ has norm 65
- → one of $\pm i(2 \pm i)(2 \pm 3i)$ equals $(-4 + 7i)$

We obtain $i(2 - i)(2 + 3i) = -4 + 7i$

Example in $\mathbb{Z}[i]$: collecting relations

$a+bi$	$aV+bU=$ factor in $\mathbb{Z}$	a^2+b^2	factor in $\mathbb{Z}[i]$
$-17+19i$	$-7=-7$	$650=2\cdot 5^2\cdot 13$	$-(1-i)(2+i)^2(2-3i)$
$-11+2i$	$-231=-3\cdot 7\cdot 11$	$125=5^3$	$i(2+i)^3$
$-6+17i$	$224=2^5\cdot 7$	$325=5^2\cdot 13$	$(2+i)^2(2+3i)$
$-4+7i$	$54=2\cdot 3^3$	$65=5\cdot 13$	$i(2-i)(2+3i)$
$-3+4i$	$13=13$	$25=5^2$	$-(2-i)^2$
$-2+i$	$-28=-2^2\cdot 7$	$5=5$	$-(2-i)$
$-2+3i$	$16=2^4$	$13=13$	$-(2-3i)$
$-2+11i$	$192=2^6\cdot 3$	$125=5^3$	$-(2-i)^3$
$-1+i$	$-3=-3$	$2=2$	$-(1-i)$
i	$22=2\cdot 11$	$1=1$	i
$1+3i$	$91=7\cdot 13$	$10=2\cdot 5$	$(1+i)(2+i)$
$1+5i$	$135=3^3\cdot 5$	$26=2\cdot 13$	$-(1-i)(2-3i)$
$2+i$	$72=2^3\cdot 3^2$	$5=5$	$(2+i)$
$5+i$	$147=3\cdot 7^2$	$26=2\cdot 13$	$-i(1+i)(2+3i)$

where $-20\le a\le 20$, $1\le b\le 20$

Example in $\mathbb{Z}[i]$: Matrix

Build the matrix of relations:

- one row per (a, b) pair s.t. both norms are smooth
- one column per prime of $\mathcal{F}_{\text{rat}}$
- one column for $1/V$
- one column per prime ideal of $\mathcal{F}_{\text{alg}}$
- one column per unit $(-1, i)$
- store the exponents

Example in $\mathbb{Z}[i]$: Matrix

Build the matrix of relations:

- one row per (a, b) pair s.t. both norms are smooth
- one column per prime of $\mathcal{F}_{\text{rat}}$
- one column for $1/V$
- one column per prime ideal of $\mathcal{F}_{\text{alg}}$
- one column per unit $(-1, i)$
- store the exponents
- change the signs of all the exponents of one side so that

$$\sum \log p_i = \sum \log q_i \iff \sum \log p_i - \sum \log q_i = 0$$

Example in $\mathbb{Z}[i]$

$M =$

2	3	5	7	11	13	$\frac{1}{V}$	-1	i	$1+i$	$1-i$	$2+i$	$2-i$	$2+3i$	$2-3i$
0	0	0	0	0	0	0	1	2	0	0	0	0	0	0
0	0	0	1	0	0	1	0	0	0	1	2	0	0	1
0	1	0	1	1	0	1	1	1	0	0	3	0	0	0
5	0	0	1	0	0	1	0	0	0	0	2	0	1	0
1	3	0	0	0	0	1	0	1	0	0	0	1	1	0
0	0	0	0	0	1	1	1	0	0	0	0	2	0	0
2	0	0	1	0	0	1	0	0	0	0	0	1	0	0
4	0	0	0	0	0	1	1	0	0	0	0	0	0	1
6	1	0	0	0	0	1	1	0	0	0	0	3	0	0
0	1	0	0	0	0	1	0	0	0	1	0	0	0	0
1	0	0	0	1	0	1	0	1	0	0	0	0	0	0
0	0	0	1	0	1	1	0	0	1	0	1	0	0	0
0	3	1	0	0	0	1	1	0	0	1	0	0	0	1
3	2	0	0	0	0	1	0	0	0	0	1	0	0	0
0	1	0	2	0	0	1	1	1	1	0	0	0	1	0

Example in $\mathbb{Z}[i]$

$$
\begin{array}{ccccccccccccccc}
2 & 3 & 5 & 7 & 11 & 13 & \frac{1}{V} & -1 & i & 1+i & 1-i & 2+i & 2-i & 2+3i & 2-3i
\end{array}
$$

$$
M = \begin{bmatrix}
 & & & & & & & 1 & 2 & & & & & & \\
 & & & 1 & & & 1 & & & & 1 & 2 & & & 1 \\
 & 1 & & 1 & 1 & & 1 & 1 & 1 & & & 3 & & & \\
5 & & & 1 & & & 1 & & & & & 2 & & 1 & \\
1 & 3 & & & & & 1 & & 1 & & & & 1 & 1 & \\
 & & & & & 1 & 1 & 1 & & & & & 2 & & \\
2 & & & 1 & & & 1 & & & & & & 1 & & \\
4 & & & & & & 1 & 1 & & & & & & & 1 \\
6 & 1 & & & & & 1 & 1 & & & & & 3 & & \\
 & 1 & & & & & 1 & & & & 1 & & & & \\
1 & & & & 1 & & 1 & & 1 & & & & & & \\
 & & & 1 & & 1 & 1 & & & 1 & & 1 & & & \\
 & 3 & 1 & & & & 1 & 1 & & & 1 & & & & 1 \\
3 & 2 & & & & & 1 & & & & & 1 & & & \\
 & 1 & & 2 & & & 1 & 1 & 1 & 1 & & & & 1 &
\end{bmatrix}
$$

Example in $\mathbb{Z}[i]$

$$
\begin{array}{c}
\\
M =
\end{array}
\begin{array}{c}
\begin{array}{ccccccccccccccc}
2 & 3 & 5 & 7 & 11 & 13 & \frac{1}{V} & -1 & i & 1+i & 1-i & 2+i & 2-i & 2+3i & 2-3i
\end{array}
\\
\left[\begin{array}{ccccccccccccccc}
 & & & & & & & -1 & -2 & & & & & & \\
 & & & 1 & & & 1 & & & & -1 & -2 & & & -1 \\
 & 1 & & 1 & 1 & & 1 & -1 & -1 & & & -3 & & & \\
5 & & & 1 & & & 1 & & & & & -2 & & -1 & \\
1 & 3 & & & & & 1 & & -1 & & & & -1 & -1 & \\
 & & & & & 1 & 1 & -1 & & & & & -2 & & \\
2 & & & 1 & & & 1 & & & & & & -1 & & \\
4 & & & & & & 1 & -1 & & & & & & & -1 \\
6 & 1 & & & & & 1 & -1 & & & & & -3 & & \\
 & 1 & & & & & 1 & & & & -1 & & & & \\
1 & & & & 1 & & 1 & & -1 & & & & & & \\
 & & & 1 & & 1 & 1 & & & -1 & & -1 & & & \\
 & 3 & 1 & & & & 1 & -1 & & & -1 & & & & -1 \\
3 & 2 & & & & & 1 & & & & & -1 & & & \\
 & 1 & & 2 & & & 1 & -1 & -1 & -1 & & & & -1 &
\end{array}\right]
\end{array}
$$

Example in $\mathbb{Z}[i]$

Right kernel $M \cdot \boldsymbol{x} = 0 \bmod (p-1)/4 = 277$:

$$\boldsymbol{x} = (\underbrace{1, 219, 40, 34, 79, 269}_{\text{rational side}}, \underbrace{197}_{1/V}, \underbrace{0, 0}_{\text{units}}, \underbrace{139, 139, 84, 233, 68, 201}_{\text{algebraic side}})$$

Logarithms (in some basis)

Rational side: logarithms of $\{2, 3, 5, 7, 11, 13\}$

$\rightarrow \log x_i / \log 2$

$\boldsymbol{x} = [1, 219, 40, 34, 79, 269] \bmod 277$

$\rightarrow$ order 4 subgroup

$\boldsymbol{v} = [1, 219, 594, 311, 910, 1100] \bmod p - 1$

Target 314, generator $g = 2$

$g^2 \cdot 314 = 147 = 3 \cdot 7^2$

$\log_g 314 = \log_g 3 + 2 \log_g 7 - 2 = 219 + 2 \cdot 311 - 2 = 839 \bmod p - 1$

$2^{839} = 314 \bmod p$

$\log_g 314 = 839$

Example in $\mathbb{Z}[i]$

$$\boldsymbol{x} = (\underbrace{1, 219, 40, 34, 79, 269}_{\text{rational side}}, \underbrace{197}_{1/V}, \underbrace{0, 0}_{\text{units}}, \underbrace{\mathbf{139}, \mathbf{139}, 84, 233, 68, 201}_{\text{algebraic side}})$$

Remark

$\log(1+i) = \log(1-i)$ because $-i(1+i) = 1-i$
and $\log(-1) = \log i = 0$
In fact, $\log$ (torsion unit) $= 0$

It would have been possible to remove $1-i$ from $\mathcal{F}_f$,
and remove the column of $1-i$ from M.

Sieve: Coppersmith–Odlyzko–Schroeppel 1986

Sieve: faster smoothness tests

Erathostene sieve: remaining numbers are prime
COS sieve: remaining numbers are not smooth: discard them

1. initialize a tabular T of norms (values $aV + bU$)
   $T[a + A][b - 1] = aV + bU$
2. sieve for q^s, $q \in \{2, 3, 5, 7, 11, 13\}$
3. cells $T[a + A][b - 1] \in \{-1, 1\}$ mean smooth $aV + bU$

Numerical example follows.

$a \in [-A, A]$, $b \in [1, A]$

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
-17	-403	-381	-359	-337	-315	-293	-271	-249	-227	-205	-183	-161	-139	-117	-95	-73	0	-29	-7	15	37
-16	-378	0	-334	0	-290	0	-246	0	-202	0	-158	0	-114	0	-70	0	-26	0	18	0	62
-15	-353	-331	0	-287	0	0	-221	-199	0	0	-133	0	-89	-67	0	-23	-1	0	43	0	0
-14	-328	0	-284	0	-240	0	0	0	-152	0	-108	0	-64	0	-20	0	24	0	68	0	0
-13	-303	-281	-259	-237	-215	-193	-171	-149	-127	-105	-83	-61	0	-17	5	27	49	71	93	115	137
-12	-278	0	0	0	-190	0	-146	0	0	0	-58	0	-14	0	0	0	74	0	118	0	0
-11	-253	-231	-209	-187	-165	-143	-121	-99	-77	-55	0	-11	11	33	55	77	99	121	143	165	187
-10	-228	0	-184	0	0	0	-96	0	-52	0	-8	0	36	0	0	0	124	0	168	0	212
-9	-203	-181	0	-137	-115	0	-71	-49	0	-5	17	0	61	83	0	127	149	0	193	215	0
-8	-178	0	-134	0	-90	0	-46	0	-2	0	42	0	86	0	130	0	174	0	218	0	262
-7	-153	-131	-109	-87	-65	-43	0	1	23	45	67	89	111	0	155	177	199	221	243	265	0
-6	-128	0	0	0	-40	0	4	0	0	0	92	0	136	0	0	0	224	0	268	0	0
-5	-103	-81	-59	-37	0	7	29	51	73	0	117	139	161	183	0	227	249	271	293	0	337
-4	-78	0	-34	0	10	0	54	0	98	0	142	0	186	0	230	0	274	0	318	0	362
-3	-53	-31	0	13	35	0	79	101	0	145	167	0	211	233	0	277	299	0	343	365	0
-2	-28	0	16	0	60	0	104	0	148	0	192	0	236	0	280	0	324	0	368	0	412
-1	-3	19	41	63	85	107	129	151	173	195	217	239	261	283	305	327	349	371	393	415	437
0	22	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	47	69	91	113	135	157	179	201	223	245	267	289	311	333	355	377	399	421	443	465	487
2	72	0	116	0	160	0	204	0	248	0	292	0	336	0	380	0	424	0	468	0	512
3	97	119	0	163	185	0	229	251	0	295	317	0	361	383	0	427	449	0	493	515	0
4	122	0	166	0	210	0	254	0	298	0	342	0	386	0	430	0	474	0	518	0	562
5	147	169	191	213	0	257	279	301	323	0	367	389	411	433	0	477	499	521	543	0	587
6	172	0	0	0	260	0	304	0	0	0	392	0	436	0	0	0	524	0	568	0	0
7	197	219	241	263	285	307	0	351	373	395	417	439	461	0	505	527	549	571	593	615	0
8	222	0	266	0	310	0	354	0	398	0	442	0	486	0	530	0	574	0	618	0	662
9	247	269	0	313	335	0	379	401	0	445	467	0	511	533	0	577	599	0	643	665	0
10	272	0	316	0	0	0	404	0	448	0	492	0	536	0	0	0	624	0	668	0	712
11	297	319	341	363	385	407	429	451	473	495	0	539	561	583	605	627	649	671	693	715	737
12	322	0	0	0	410	0	454	0	0	0	542	0	586	0	0	0	674	0	718	0	0
13	347	369	391	413	435	457	479	501	523	545	567	589	0	633	655	677	699	721	743	765	787
14	372	0	416	0	460	0	0	0	548	0	592	0	636	0	680	0	724	0	768	0	0
15	397	419	0	463	0	0	529	551	0	0	617	0	661	683	0	727	749	0	793	0	0
16	422	0	466	0	510	0	554	0	598	0	642	0	686	0	730	0	774	0	818	0	862
17	447	469	491	513	535	557	579	601	623	645	667	689	711	733	755	777	0	821	843	865	887

$\gcd(a, b) = 1$

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
-17	-403	-381	-359	-337	-315	-293	-271	-249	-227	-205	-183	-161	-139	-117	-95	-73		-29	-7	15	37
-16	-378		-334		-290		-246		-202		-158		-114		-70		-26		18		62
-15	-353	-331		-287			-221	-199			-133		-89	-67		-23	-1		43		
-14	-328		-284		-240				-152		-108		-64		-20		24		68		
-13	-303	-281	-259	-237	-215	-193	-171	-149	-127	-105	-83	-61		-17	5	27	49	71	93	115	137
-12	-278				-190		-146				-58		-14				74		118		
-11	-253	-231	-209	-187	-165	-143	-121	-99	-77	-55		-11	11	33	55	77	99	121	143	165	187
-10	-228		-184				-96		-52		-8		36				124		168		212
-9	-203	-181		-137	-115		-71	-49		-5	17		61	83		127	149		193	215	
-8	-178		-134		-90		-46		-2		42		86		130		174		218		262
-7	-153	-131	-109	-87	-65	-43		1	23	45	67	89	111		155	177	199	221	243	265	
-6	-128				-40		4				92		136				224		268		
-5	-103	-81	-59	-37		7	29	51	73		117	139	161	183		227	249	271	293		337
-4	-78		-34		10		54		98		142		186		230		274		318		362
-3	-53	-31		13	35		79	101		145	167		211	233		277	299		343	365	
-2	-28		16		60		104		148		192		236		280		324		368		412
-1	-3	19	41	63	85	107	129	151	173	195	217	239	261	283	305	327	349	371	393	415	437
0	22																				
1	47	69	91	113	135	157	179	201	223	245	267	289	311	333	355	377	399	421	443	465	487
2	72		116		160		204		248		292		336		380		424		468		512
3	97	119		163	185		229	251		295	317		361	383		427	449		493	515	
4	122		166		210		254		298		342		386		430		474		518		562
5	147	169	191	213		257	279	301	323		367	389	411	433		477	499	521	543		587
6	172				260		304				392		436				524		568		
7	197	219	241	263	285	307		351	373	395	417	439	461		505	527	549	571	593	615	
8	222		266		310		354		398		442		486		530		574		618		662
9	247	269		313	335		379	401		445	467		511	533		577	599		643	665	
10	272		316				404		448		492		536				624		668		712
11	297	319	341	363	385	407	429	451	473	495		539	561	583	605	627	649	671	693	715	737
12	322				410		454				542		586				674		718		
13	347	369	391	413	435	457	479	501	523	545	567	589		633	655	677	699	721	743	765	787
14	372		416		460				548		592		636		680		724		768		
15	397	419		463			529	551			617		661	683		727	749		793		
16	422		466		510		554		598		642		686		730		774		818		862
17	447	469	491	513	535	557	579	601	623	645	667	689	711	733	755	777		821	843	865	887

$q = 2$, $Va + Ub = 25a + 22b$

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
-17	-403	-381	-359	-337	-315	-293	-271	-249	-227	-205	-183	-161	-139	-117	-95	-73		-29	-7	15	37
-16	-378		-334		-290		-246		-202		-158		-114		-70		-26		18		62
-15	-353	-331		-287			-221	-199			-133		-89	-67		-23	-1		43		
-14	-328		-284		-240				-152		-108		-64		-20		24		68		
-13	-303	-281	-259	-237	-215	-193	-171	-149	-127	-105	-83	-61		-17	5	27	49	71	93	115	137
-12	-278				-190		-146				-58		-14				74		118		
-11	-253	-231	-209	-187	-165	-143	-121	-99	-77	-55		-11	11	33	55	77	99	121	143	165	187
-10	-228		-184				-96		-52		-8		36				124		168		212
-9	-203	-181		-137	-115		-71	-49		-5	17		61	83		127	149		193	215	
-8	-178		-134		-90		-46		-2		42		86		130		174		218		262
-7	-153	-131	-109	-87	-65	-43		1	23	45	67	89	111		155	177	199	221	243	265	
-6	-128				-40		4				92		136				224		268		
-5	-103	-81	-59	-37		7	29	51	73		117	139	161	183		227	249	271	293		337
-4	-78		-34		10		54		98		142		186		230		274		318		362
-3	-53	-31		13	35		79	101		145	167		211	233		277	299		343	365	
-2	-28		16		60		104		148		192		236		280		324		368		412
-1	-3	19	41	63	85	107	129	151	173	195	217	239	261	283	305	327	349	371	393	415	437
0	22																				
1	47	69	91	113	135	157	179	201	223	245	267	289	311	333	355	377	399	421	443	465	487
2	72		116		160		204		248		292		336		380		424		468		512
3	97	119		163	185		229	251		295	317		361	383		427	449		493	515	
4	122		166		210		254		298		342		386		430		474		518		562
5	147	169	191	213		257	279	301	323		367	389	411	433		477	499	521	543		587
6	172				260		304				392		436				524		568		
7	197	219	241	263	285	307		351	373	395	417	439	461		505	527	549	571	593	615	
8	222		266		310		354		398		442		486		530		574		618		662
9	247	269		313	335		379	401		445	467		511	533		577	599		643	665	
10	272		316				404		448		492		536				624		668		712
11	297	319	341	363	385	407	429	451	473	495		539	561	583	605	627	649	671	693	715	737
12	322				410		454				542		586				674		718		
13	347	369	391	413	435	457	479	501	523	545	567	589		633	655	677	699	721	743	765	787
14	372		416		460				548		592		636		680		724		768		
15	397	419		463			529	551			617		661	683		727	749		793		
16	422		466		510		554		598		642		686		730		774		818		862
17	447	469	491	513	535	557	579	601	623	645	667	689	711	733	755	777		821	843	865	887

$q = 2$, $Va + Ub = 25a + 22b$

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
-17	-403	-381	-359	-337	-315	-293	-271	-249	-227	-205	-183	-161	-139	-117	-95	-73		-29	-7	15	37
-16	-189		-167		-145		-123		-101		-79		-57		-35		-13		9		31
-15	-353	-331		-287			-221	-199			-133		-89	-67		-23	-1		43		
-14	-164		-142		-120				-76		-54		-32		-10		12		34		
-13	-303	-281	-259	-237	-215	-193	-171	-149	-127	-105	-83	-61		-17	5	27	49	71	93	115	137
-12	-139				-95		-73				-29		-7				37		59		
-11	-253	-231	-209	-187	-165	-143	-121	-99	-77	-55		-11	11	33	55	77	99	121	143	165	187
-10	-114		-92				-48		-26		-4		18				62		84		106
-9	-203	-181		-137	-115		-71	-49		-5	17		61	83		127	149		193	215	
-8	-89		-67		-45		-23		-1		21		43		65		87		109		131
-7	-153	-131	-109	-87	-65	-43		1	23	45	67	89	111		155	177	199	221	243	265	
-6	-64				-20		2				46		68				112		134		
-5	-103	-81	-59	-37		7	29	51	73		117	139	161	183		227	249	271	293		337
-4	-39		-17		5		27		49		71		93		115		137		159		181
-3	-53	-31		13	35		79	101		145	167		211	233		277	299		343	365	
-2	-14		8		30		52		74		96		118		140		162		184		206
-1	-3	19	41	63	85	107	129	151	173	195	217	239	261	283	305	327	349	371	393	415	437
0	11																				
1	47	69	91	113	135	157	179	201	223	245	267	289	311	333	355	377	399	421	443	465	487
2	36		58		80		102		124		146		168		190		212		234		256
3	97	119		163	185		229	251		295	317		361	383		427	449		493	515	
4	61		83		105		127		149		171		193		215		237		259		281
5	147	169	191	213		257	279	301	323		367	389	411	433		477	499	521	543		587
6	86				130		152				196		218				262		284		
7	197	219	241	263	285	307		351	373	395	417	439	461		505	527	549	571	593	615	
8	111		133		155		177		199		221		243		265		287		309		331
9	247	269		313	335		379	401		445	467		511	533		577	599		643	665	
10	136		158				202		224		246		268				312		334		356
11	297	319	341	363	385	407	429	451	473	495		539	561	583	605	627	649	671	693	715	737
12	161				205		227				271		293				337		359		
13	347	369	391	413	435	457	479	501	523	545	567	589		633	655	677	699	721	743	765	787
14	186		208		230				274		296		318		340		362		384		
15	397	419		463			529	551			617		661	683		727	749		793		
16	211		233		255		277		299		321		343		365		387		409		431
17	447	469	491	513	535	557	579	601	623	645	667	689	711	733	755	777		821	843	865	887

$q = 2^2$, $Va + Ub = 25a + 22b$

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
-17	-403	-381	-359	-337	-315	-293	-271	-249	-227	-205	-183	-161	-139	-117	-95	-73		-29	-7	15	37
-16	-189		-167		-145		-123		-101		-79		-57		-35		-13		9		31
-15	-353	-331		-287			-221	-199			-133		-89	-67		-23	-1		43		
-14	-164		-142		-120				-76		-54		-32		-10		12		34		
-13	-303	-281	-259	-237	-215	-193	-171	-149	-127	-105	-83	-61		-17	5	27	49	71	93	115	137
-12	-139				-95		-73				-29		-7				37		59		
-11	-253	-231	-209	-187	-165	-143	-121	-99	-77	-55		-11	11	33	55	77	99	121	143	165	187
-10	-114		-92				-48		-26		-4		18				62		84		106
-9	-203	-181		-137	-115		-71	-49		-5	17		61	83		127	149		193	215	
-8	-89		-67		-45		-23		-1		21		43		65		87		109		131
-7	-153	-131	-109	-87	-65	-43		1	23	45	67	89	111		155	177	199	221	243	265	
-6	-64				-20		2				46		68				112		134		
-5	-103	-81	-59	-37		7	29	51	73		117	139	161	183		227	249	271	293		337
-4	-39		-17		5		27		49		71		93		115		137		159		181
-3	-53	-31		13	35		79	101		145	167		211	233		277	299		343	365	
-2	-14		8		30		52		74		96		118		140		162		184		206
-1	-3	19	41	63	85	107	129	151	173	195	217	239	261	283	305	327	349	371	393	415	437
0	11																				
1	47	69	91	113	135	157	179	201	223	245	267	289	311	333	355	377	399	421	443	465	487
2	36		58		80		102		124		146		168		190		212		234		256
3	97	119		163	185		229	251		295	317		361	383		427	449		493	515	
4	61		83		105		127		149		171		193		215		237		259		281
5	147	169	191	213		257	279	301	323		367	389	411	433		477	499	521	543		587
6	86				130		152				196		218				262		284		
7	197	219	241	263	285	307		351	373	395	417	439	461		505	527	549	571	593	615	
8	111		133		155		177		199		221		243		265		287		309		331
9	247	269		313	335		379	401		445	467		511	533		577	599		643	665	
10	136		158				202		224		246		268				312		334		356
11	297	319	341	363	385	407	429	451	473	495		539	561	583	605	627	649	671	693	715	737
12	161				205		227				271		293				337		359		
13	347	369	391	413	435	457	479	501	523	545	567	589		633	655	677	699	721	743	765	787
14	186		208		230				274		296		318		340		362		384		
15	397	419		463			529	551			617		661	683		727	749		793		
16	211		233		255		277		299		321		343		365		387		409		431
17	447	469	491	513	535	557	579	601	623	645	667	689	711	733	755	777		821	843	865	887

$q = 2^2$, $Va + Ub = 25a + 22b$

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
-17	-403	-381	-359	-337	-315	-293	-271	-249	-227	-205	-183	-161	-139	-117	-95	-73		-29	-7	15	37
-16	-189		-167		-145		-123		-101		-79		-57		-35		-13		9		31
-15	-353	-331		-287			-221	-199			-133		-89	-67		-23	-1		43		
-14	-82		-71		-60				-38		-27		-16		-5		6		17		
-13	-303	-281	-259	-237	-215	-193	-171	-149	-127	-105	-83	-61		-17	5	27	49	71	93	115	137
-12	-139				-95		-73				-29		-7				37		59		
-11	-253	-231	-209	-187	-165	-143	-121	-99	-77	-55		-11	11	33	55	77	99	121	143	165	187
-10	-57		-46				-24		-13		-2		9				31		42		53
-9	-203	-181		-137	-115		-71	-49		-5	17		61	83		127	149		193	215	
-8	-89		-67		-45		-23		-1		21		43		65		87		109		131
-7	-153	-131	-109	-87	-65	-43		1	23	45	67	89	111		155	177	199	221	243	265	
-6	-32				-10		1				23		34				56		67		
-5	-103	-81	-59	-37		7	29	51	73		117	139	161	183		227	249	271	293		337
-4	-39		-17		5		27		49		71		93		115		137		159		181
-3	-53	-31		13	35		79	101		145	167		211	233		277	299		343	365	
-2	-7		4		15		26		37		48		59		70		81		92		103
-1	-3	19	41	63	85	107	129	151	173	195	217	239	261	283	305	327	349	371	393	415	437
0	11																				
1	47	69	91	113	135	157	179	201	223	245	267	289	311	333	355	377	399	421	443	465	487
2	18		29		40		51		62		73		84		95		106		117		128
3	97	119		163	185		229	251		295	317		361	383		427	449		493	515	
4	61		83		105		127		149		171		193		215		237		259		281
5	147	169	191	213		257	279	301	323		367	389	411	433		477	499	521	543		587
6	43				65		76				98		109				131		142		
7	197	219	241	263	285	307		351	373	395	417	439	461		505	527	549	571	593	615	
8	111		133		155		177		199		221		243		265		287		309		331
9	247	269		313	335		379	401		445	467		511	533		577	599		643	665	
10	68		79				101		112		123		134				156		167		178
11	297	319	341	363	385	407	429	451	473	495		539	561	583	605	627	649	671	693	715	737
12	161				205		227				271		293				337		359		
13	347	369	391	413	435	457	479	501	523	545	567	589		633	655	677	699	721	743	765	787
14	93		104		115				137		148		159		170		181		192		
15	397	419		463			529	551			617		661	683		727	749		793		
16	211		233		255		277		299		321		343		365		387		409		431
17	447	469	491	513	535	557	579	601	623	645	667	689	711	733	755	777		821	843	865	887

$q = 2^3$, $Va + Ub = 25a + 22b$

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
-17	-403	-381	-359	-337	-315	-293	-271	-249	-227	-205	-183	-161	-139	-117	-95	-73		-29	-7	15	37
-16	-189		-167		-145		-123		-101		-79		-57		-35		-13		9		31
-15	-353	-331		-287			-221	-199			-133		-89	-67		-23	-1		43		
-14	-82		-71		-60				-38		-27		-16		-5		6		17		
-13	-303	-281	-259	-237	-215	-193	-171	-149	-127	-105	-83	-61		-17	5	27	49	71	93	115	137
-12	-139				-95		-73				-29		-7				37		59		
-11	-253	-231	-209	-187	-165	-143	-121	-99	-77	-55		-11	11	33	55	77	99	121	143	165	187
-10	-57		-46				-24		-13		-2		9				31		42		53
-9	-203	-181		-137	-115		-71	-49		-5	17		61	83		127	149		193	215	
-8	-89		-67		-45		-23		-1		21		43		65		87		109		131
-7	-153	-131	-109	-87	-65	-43		1	23	45	67	89	111		155	177	199	221	243	265	
-6	-32				-10		1				23		34				56		67		
-5	-103	-81	-59	-37		7	29	51	73		117	139	161	183		227	249	271	293		337
-4	-39		-17		5		27		49		71		93		115		137		159		181
-3	-53	-31		13	35		79	101		145	167		211	233		277	299		343	365	
-2	-7		4		15		26		37		48		59		70		81		92		103
-1	-3	19	41	63	85	107	129	151	173	195	217	239	261	283	305	327	349	371	393	415	437
0	11																				
1	47	69	91	113	135	157	179	201	223	245	267	289	311	333	355	377	399	421	443	465	487
2	18		29		40		51		62		73		84		95		106		117		128
3	97	119		163	185		229	251		295	317		361	383		427	449		493	515	
4	61		83		105		127		149		171		193		215		237		259		281
5	147	169	191	213		257	279	301	323		367	389	411	433		477	499	521	543		587
6	43				65		76				98		109				131		142		
7	197	219	241	263	285	307		351	373	395	417	439	461		505	527	549	571	593	615	
8	111		133		155		177		199		221		243		265		287		309		331
9	247	269		313	335		379	401		445	467		511	533		577	599		643	665	
10	68		79				101		112		123		134				156		167		178
11	297	319	341	363	385	407	429	451	473	495		539	561	583	605	627	649	671	693	715	737
12	161				205		227				271		293				337		359		
13	347	369	391	413	435	457	479	501	523	545	567	589		633	655	677	699	721	743	765	787
14	93		104		115				137		148		159		170		181		192		
15	397	419		463			529	551			617		661	683		727	749		793		
16	211		233		255		277		299		321		343		365		387		409		431
17	447	469	491	513	535	557	579	601	623	645	667	689	711	733	755	777		821	843	865	887

$q = 2^3$, $Va + Ub = 25a + 22b$

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
-17	-403	-381	-359	-337	-315	-293	-271	-249	-227	-205	-183	-161	-139	-117	-95	-73		-29	-7	15	37
-16	-189		-167		-145		-123		-101		-79		-57		-35		-13		9		31
-15	-353	-331		-287			-221	-199			-133		-89	-67		-23	-1		43		
-14	-41		-71		-30				-19		-27		-8		-5		3		17		
-13	-303	-281	-259	-237	-215	-193	-171	-149	-127	-105	-83	-61		-17	5	27	49	71	93	115	137
-12	-139				-95		-73				-29		-7				37		59		
-11	-253	-231	-209	-187	-165	-143	-121	-99	-77	-55		-11	11	33	55	77	99	121	143	165	187
-10	-57		-23				-12		-13		-1		9				31		21		53
-9	-203	-181		-137	-115		-71	-49		-5	17		61	83		127	149		193	215	
-8	-89		-67		-45		-23		-1		21		43		65		87		109		131
-7	-153	-131	-109	-87	-65	-43		1	23	45	67	89	111		155	177	199	221	243	265	
-6	-16				-5		1				23		17				28		67		
-5	-103	-81	-59	-37		7	29	51	73		117	139	161	183		227	249	271	293		337
-4	-39		-17		5		27		49		71		93		115		137		159		181
-3	-53	-31		13	35		79	101		145	167		211	233		277	299		343	365	
-2	-7		2		15		13		37		24		59		35		81		46		103
-1	-3	19	41	63	85	107	129	151	173	195	217	239	261	283	305	327	349	371	393	415	437
0	11																				
1	47	69	91	113	135	157	179	201	223	245	267	289	311	333	355	377	399	421	443	465	487
2	9		29		20		51		31		73		42		95		53		117		64
3	97	119		163	185		229	251		295	317		361	383		427	449		493	515	
4	61		83		105		127		149		171		193		215		237		259		281
5	147	169	191	213		257	279	301	323		367	389	411	433		477	499	521	543		587
6	43				65		38				49		109				131		71		
7	197	219	241	263	285	307		351	373	395	417	439	461		505	527	549	571	593	615	
8	111		133		155		177		199		221		243		265		287		309		331
9	247	269		313	335		379	401		445	467		511	533		577	599		643	665	
10	34		79				101		56		123		67				78		167		89
11	297	319	341	363	385	407	429	451	473	495		539	561	583	605	627	649	671	693	715	737
12	161				205		227				271		293				337		359		
13	347	369	391	413	435	457	479	501	523	545	567	589		633	655	677	699	721	743	765	787
14	93		52		115				137		74		159		85		181		96		
15	397	419		463			529	551			617		661	683		727	749		793		
16	211		233		255		277		299		321		343		365		387		409		431
17	447	469	491	513	535	557	579	601	623	645	667	689	711	733	755	777		821	843	865	887

$q = 2^4,\ Va + Ub = 25a + 22b$

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
-17	-403	-381	-359	-337	-315	-293	-271	-249	-227	-205	-183	-161	-139	-117	-95	-73		-29	-7	15	37
-16	-189		-167		-145		-123		-101		-79		-57		-35		-13		9		31
-15	-353	-331		-287			-221	-199			-133		-89	-67		-23	-1		43		
-14	-41		-71		-30				-19		-27		-8		-5		3		17		
-13	-303	-281	-259	-237	-215	-193	-171	-149	-127	-105	-83	-61		-17	5	27	49	71	93	115	137
-12	-139				-95		-73				-29		-7				37		59		
-11	-253	-231	-209	-187	-165	-143	-121	-99	-77	-55		-11	11	33	55	77	99	121	143	165	187
-10	-57		-23				-12		-13		-1		9				31		21		53
-9	-203	-181		-137	-115		-71	-49		-5	17		61	83		127	149		193	215	
-8	-89		-67		-45		-23		-1		21		43		65		87		109		131
-7	-153	-131	-109	-87	-65	-43		1	23	45	67	89	111		155	177	199	221	243	265	
-6	-16				-5		1				23		17				28		67		
-5	-103	-81	-59	-37		7	29	51	73		117	139	161	183		227	249	271	293		337
-4	-39		-17		5		27		49		71		93		115		137		159		181
-3	-53	-31		13	35		79	101		145	167		211	233		277	299		343	365	
-2	-7		2		15		13		37		24		59		35		81		46		103
-1	-3	19	41	63	85	107	129	151	173	195	217	239	261	283	305	327	349	371	393	415	437
0	11																				
1	47	69	91	113	135	157	179	201	223	245	267	289	311	333	355	377	399	421	443	465	487
2	9		29		20		51		31		73		42		95		53		117		64
3	97	119		163	185		229	251		295	317		361	383		427	449		493	515	
4	61		83		105		127		149		171		193		215		237		259		281
5	147	169	191	213		257	279	301	323		367	389	411	433		477	499	521	543		587
6	43				65		38				49		109				131		71		
7	197	219	241	263	285	307		351	373	395	417	439	461		505	527	549	571	593	615	
8	111		133		155		177		199		221		243		265		287		309		331
9	247	269		313	335		379	401		445	467		511	533		577	599		643	665	
10	34		79				101		56		123		67				78		167		89
11	297	319	341	363	385	407	429	451	473	495		539	561	583	605	627	649	671	693	715	737
12	161				205		227				271		293				337		359		
13	347	369	391	413	435	457	479	501	523	545	567	589		633	655	677	699	721	743	765	787
14	93		52		115				137		74		159		85		181		96		
15	397	419		463			529	551			617		661	683		727	749		793		
16	211		233		255		277		299		321		343		365		387		409		431
17	447	469	491	513	535	557	579	601	623	645	667	689	711	733	755	777		821	843	865	887

$q = 2^4$, $Va + Ub = 25a + 22b$

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
-17	-403	-381	-359	-337	-315	-293	-271	-249	-227	-205	-183	-161	-139	-117	-95	-73		-29	-7	15	37
-16	-189		-167		-145		-123		-101		-79		-57		-35		-13		9		31
-15	-353	-331		-287			-221	-199			-133		-89	-67		-23	-1		43		
-14	-41		-71		-15				-19		-27		-4		-5		3		17		
-13	-303	-281	-259	-237	-215	-193	-171	-149	-127	-105	-83	-61		-17	5	27	49	71	93	115	137
-12	-139				-95		-73				-29		-7				37		59		
-11	-253	-231	-209	-187	-165	-143	-121	-99	-77	-55		-11	11	33	55	77	99	121	143	165	187
-10	-57		-23				-6		-13		-1		9				31		21		53
-9	-203	-181		-137	-115		-71	-49		-5	17		61	83		127	149		193	215	
-8	-89		-67		-45		-23		-1		21		43		65		87		109		131
-7	-153	-131	-109	-87	-65	-43		1	23	45	67	89	111		155	177	199	221	243	265	
-6	-8				-5		1				23		17				14		67		
-5	-103	-81	-59	-37		7	29	51	73		117	139	161	183		227	249	271	293		337
-4	-39		-17		5		27		49		71		93		115		137		159		181
-3	-53	-31		13	35		79	101		145	167		211	233		277	299		343	365	
-2	-7		1		15		13		37		12		59		35		81		23		103
-1	-3	19	41	63	85	107	129	151	173	195	217	239	261	283	305	327	349	371	393	415	437
0	11																				
1	47	69	91	113	135	157	179	201	223	245	267	289	311	333	355	377	399	421	443	465	487
2	9		29		10		51		31		73		21		95		53		117		32
3	97	119		163	185		229	251		295	317		361	383		427	449		493	515	
4	61		83		105		127		149		171		193		215		237		259		281
5	147	169	191	213		257	279	301	323		367	389	411	433		477	499	521	543		587
6	43				65		19				49		109				131		71		
7	197	219	241	263	285	307		351	373	395	417	439	461		505	527	549	571	593	615	
8	111		133		155		177		199		221		243		265		287		309		331
9	247	269		313	335		379	401		445	467		511	533		577	599		643	665	
10	17		79				101		28		123		67				39		167		89
11	297	319	341	363	385	407	429	451	473	495		539	561	583	605	627	649	671	693	715	737
12	161				205		227				271		293				337		359		
13	347	369	391	413	435	457	479	501	523	545	567	589		633	655	677	699	721	743	765	787
14	93		26		115				137		37		159		85		181		48		
15	397	419		463			529	551			617		661	683		727	749		793		
16	211		233		255		277		299		321		343		365		387		409		431
17	447	469	491	513	535	557	579	601	623	645	667	689	711	733	755	777		821	843	865	887

$q = 2^5$, $Va + Ub = 25a + 22b$

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
-17	-403	-381	-359	-337	-315	-293	-271	-249	-227	-205	-183	-161	-139	-117	-95	-73		-29	-7	15	37
-16	-189		-167		-145		-123		-101		-79		-57		-35		-13		9		31
-15	-353	-331		-287			-221	-199			-133		-89	-67		-23	-1		43		
-14	-41		-71		-15				-19		-27		-4		-5		3		17		
-13	-303	-281	-259	-237	-215	-193	-171	-149	-127	-105	-83	-61		-17	5	27	49	71	93	115	137
-12	-139				-95		-73				-29		-7				37		59		
-11	-253	-231	-209	-187	-165	-143	-121	-99	-77	-55		-11	11	33	55	77	99	121	143	165	187
-10	-57		-23				-6		-13		-1		9				31		21		53
-9	-203	-181		-137	-115		-71	-49		-5	17		61	83		127	149		193	215	
-8	-89		-67		-45		-23		-1		21		43		65		87		109		131
-7	-153	-131	-109	-87	-65	-43		1	23	45	67	89	111		155	177	199	221	243	265	
-6	-8				-5		1				23		17				14		67		
-5	-103	-81	-59	-37		7	29	51	73		117	139	161	183		227	249	271	293		337
-4	-39		-17		5		27		49		71		93		115		137		159		181
-3	-53	-31		13	35		79	101		145	167		211	233		277	299		343	365	
-2	-7		1		15		13		37		12		59		35		81		23		103
-1	-3	19	41	63	85	107	129	151	173	195	217	239	261	283	305	327	349	371	393	415	437
0	11																				
1	47	69	91	113	135	157	179	201	223	245	267	289	311	333	355	377	399	421	443	465	487
2	9		29		10		51		31		73		21		95		53		117		32
3	97	119		163	185		229	251		295	317		361	383		427	449		493	515	
4	61		83		105		127		149		171		193		215		237		259		281
5	147	169	191	213		257	279	301	323		367	389	411	433		477	499	521	543		587
6	43				65		19				49		109				131		71		
7	197	219	241	263	285	307		351	373	395	417	439	461		505	527	549	571	593	615	
8	111		133		155		177		199		221		243		265		287		309		331
9	247	269		313	335		379	401		445	467		511	533		577	599		643	665	
10	17		79				101		28		123		67				39		167		89
11	297	319	341	363	385	407	429	451	473	495		539	561	583	605	627	649	671	693	715	737
12	161				205		227				271		293				337		359		
13	347	369	391	413	435	457	479	501	523	545	567	589		633	655	677	699	721	743	765	787
14	93		26		115				137		37		159		85		181		48		
15	397	419		463			529	551			617		661	683		727	749		793		
16	211		233		255		277		299		321		343		365		387		409		431
17	447	469	491	513	535	557	579	601	623	645	667	689	711	733	755	777		821	843	865	887

$q = 2^5$, $Va + Ub = 25a + 22b$

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
-17	-403	-381	-359	-337	-315	-293	-271	-249	-227	-205	-183	-161	-139	-117	-95	-73		-29	-7	15	37
-16	-189		-167		-145		-123		-101		-79		-57		-35		-13		9		31
-15	-353	-331		-287			-221	-199			-133		-89	-67		-23	-1		43		
-14	-41		-71		-15				-19		-27		-2		-5		3		17		
-13	-303	-281	-259	-237	-215	-193	-171	-149	-127	-105	-83	-61		-17	5	27	49	71	93	115	137
-12	-139				-95		-73				-29		-7				37		59		
-11	-253	-231	-209	-187	-165	-143	-121	-99	-77	-55		-11	11	33	55	77	99	121	143	165	187
-10	-57		-23				-3		-13		-1		9				31		21		53
-9	-203	-181		-137	-115		-71	-49		-5	17		61	83		127	149		193	215	
-8	-89		-67		-45		-23		-1		21		43		65		87		109		131
-7	-153	-131	-109	-87	-65	-43		1	23	45	67	89	111		155	177	199	221	243	265	
-6	-4				-5		1				23		17				7		67		
-5	-103	-81	-59	-37		7	29	51	73		117	139	161	183		227	249	271	293		337
-4	-39		-17		5		27		49		71		93		115		137		159		181
-3	-53	-31		13	35		79	101		145	167		211	233		277	299		343	365	
-2	-7		1		15		13		37		6		59		35		81		23		103
-1	-3	19	41	63	85	107	129	151	173	195	217	239	261	283	305	327	349	371	393	415	437
0	11																				
1	47	69	91	113	135	157	179	201	223	245	267	289	311	333	355	377	399	421	443	465	487
2	9		29		5		51		31		73		21		95		53		117		16
3	97	119		163	185		229	251		295	317		361	383		427	449		493	515	
4	61		83		105		127		149		171		193		215		237		259		281
5	147	169	191	213		257	279	301	323		367	389	411	433		477	499	521	543		587
6	43				65		19				49		109				131		71		
7	197	219	241	263	285	307		351	373	395	417	439	461		505	527	549	571	593	615	
8	111		133		155		177		199		221		243		265		287		309		331
9	247	269		313	335		379	401		445	467		511	533		577	599		643	665	
10	17		79				101		14		123		67				39		167		89
11	297	319	341	363	385	407	429	451	473	495		539	561	583	605	627	649	671	693	715	737
12	161				205		227				271		293				337		359		
13	347	369	391	413	435	457	479	501	523	545	567	589		633	655	677	699	721	743	765	787
14	93		13		115				137		37		159		85		181		24		
15	397	419		463			529	551			617		661	683		727	749		793		
16	211		233		255		277		299		321		343		365		387		409		431
17	447	469	491	513	535	557	579	601	623	645	667	689	711	733	755	777		821	843	865	887

$q = 2^6$, $Va + Ub = 25a + 22b$

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
-17	-403	-381	-359	-337	-315	-293	-271	-249	-227	-205	-183	-161	-139	-117	-95	-73		-29	-7	15	37
-16	-189		-167		-145		-123		-101		-79		-57		-35		-13		9		31
-15	-353	-331		-287			-221	-199			-133		-89	-67		-23	-1		43		
-14	-41		-71		-15				-19		-27		-2		-5		3		17		
-13	-303	-281	-259	-237	-215	-193	-171	-149	-127	-105	-83	-61		-17	5	27	49	71	93	115	137
-12	-139				-95		-73				-29		-7				37		59		
-11	-253	-231	-209	-187	-165	-143	-121	-99	-77	-55		-11	11	33	55	77	99	121	143	165	187
-10	-57		-23				-3		-13		-1		9				31		21		53
-9	-203	-181		-137	-115		-71	-49		-5	17		61	83		127	149		193	215	
-8	-89		-67		-45		-23		-1		21		43		65		87		109		131
-7	-153	-131	-109	-87	-65	-43		1	23	45	67	89	111		155	177	199	221	243	265	
-6	-4				-5		1				23		17				7		67		
-5	-103	-81	-59	-37		7	29	51	73		117	139	161	183		227	249	271	293		337
-4	-39		-17		5		27		49		71		93		115		137		159		181
-3	-53	-31		13	35		79	101		145	167		211	233		277	299		343	365	
-2	-7		1		15		13		37		6		59		35		81		23		103
-1	-3	19	41	63	85	107	129	151	173	195	217	239	261	283	305	327	349	371	393	415	437
0	11																				
1	47	69	91	113	135	157	179	201	223	245	267	289	311	333	355	377	399	421	443	465	487
2	9		29		5		51		31		73		21		95		53		117		16
3	97	119		163	185		229	251		295	317		361	383		427	449		493	515	
4	61		83		105		127		149		171		193		215		237		259		281
5	147	169	191	213		257	279	301	323		367	389	411	433		477	499	521	543		587
6	43				65		19				49		109				131		71		
7	197	219	241	263	285	307		351	373	395	417	439	461		505	527	549	571	593	615	
8	111		133		155		177		199		221		243		265		287		309		331
9	247	269		313	335		379	401		445	467		511	533		577	599		643	665	
10	17		79				101		14		123		67				39		167		89
11	297	319	341	363	385	407	429	451	473	495		539	561	583	605	627	649	671	693	715	737
12	161				205		227				271		293				337		359		
13	347	369	391	413	435	457	479	501	523	545	567	589		633	655	677	699	721	743	765	787
14	93		13		115				137		37		159		85		181		24		
15	397	419		463			529	551			617		661	683		727	749		793		
16	211		233		255		277		299		321		343		365		387		409		431
17	447	469	491	513	535	557	579	601	623	645	667	689	711	733	755	777		821	843	865	887

$q = 2^6$, $Va + Ub = 25a + 22b$

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
-17	-403	-381	-359	-337	-315	-293	-271	-249	-227	-205	-183	-161	-139	-117	-95	-73		-29	-7	15	37
-16	-189		-167		-145		-123		-101		-79		-57		-35		-13		9		31
-15	-353	-331		-287			-221	-199			-133		-89	-67		-23	-1		43		
-14	-41		-71		-15				-19		-27		-1		-5		3		17		
-13	-303	-281	-259	-237	-215	-193	-171	-149	-127	-105	-83	-61		-17	5	27	49	71	93	115	137
-12	-139				-95		-73				-29		-7				37		59		
-11	-253	-231	-209	-187	-165	-143	-121	-99	-77	-55		-11	11	33	55	77	99	121	143	165	187
-10	-57		-23				-3		-13		-1		9				31		21		53
-9	-203	-181		-137	-115		-71	-49		-5	17		61	83		127	149		193	215	
-8	-89		-67		-45		-23		-1		21		43		65		87		109		131
-7	-153	-131	-109	-87	-65	-43		1	23	45	67	89	111		155	177	199	221	243	265	
-6	-2				-5		1				23		17				7		67		
-5	-103	-81	-59	-37		7	29	51	73		117	139	161	183		227	249	271	293		337
-4	-39		-17		5		27		49		71		93		115		137		159		181
-3	-53	-31		13	35		79	101		145	167		211	233		277	299		343	365	
-2	-7		1		15		13		37		3		59		35		81		23		103
-1	-3	19	41	63	85	107	129	151	173	195	217	239	261	283	305	327	349	371	393	415	437
0	11																				
1	47	69	91	113	135	157	179	201	223	245	267	289	311	333	355	377	399	421	443	465	487
2	9		29		5		51		31		73		21		95		53		117		8
3	97	119		163	185		229	251		295	317		361	383		427	449		493	515	
4	61		83		105		127		149		171		193		215		237		259		281
5	147	169	191	213		257	279	301	323		367	389	411	433		477	499	521	543		587
6	43				65		19				49		109				131		71		
7	197	219	241	263	285	307		351	373	395	417	439	461		505	527	549	571	593	615	
8	111		133		155		177		199		221		243		265		287		309		331
9	247	269		313	335		379	401		445	467		511	533		577	599		643	665	
10	17		79				101		7		123		67				39		167		89
11	297	319	341	363	385	407	429	451	473	495		539	561	583	605	627	649	671	693	715	737
12	161				205		227				271		293				337		359		
13	347	369	391	413	435	457	479	501	523	545	567	589		633	655	677	699	721	743	765	787
14	93		13		115				137		37		159		85		181		12		
15	397	419		463			529	551			617		661	683		727	749		793		
16	211		233		255		277		299		321		343		365		387		409		431
17	447	469	491	513	535	557	579	601	623	645	667	689	711	733	755	777		821	843	865	887

$q = 2^7$, $Va + Ub = 25a + 22b$

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
-17	-403	-381	-359	-337	-315	-293	-271	-249	-227	-205	-183	-161	-139	-117	-95	-73		-29	-7	15	37
-16	-189		-167		-145		-123		-101		-79		-57		-35		-13		9		31
-15	-353	-331		-287			-221	-199			-133		-89	-67		-23	-1		43		
-14	-41		-71		-15				-19		-27		-1		-5		3		17		
-13	-303	-281	-259	-237	-215	-193	-171	-149	-127	-105	-83	-61		-17	5	27	49	71	93	115	137
-12	-139				-95		-73				-29		-7				37		59		
-11	-253	-231	-209	-187	-165	-143	-121	-99	-77	-55		-11	11	33	55	77	99	121	143	165	187
-10	-57		-23				-3		-13		-1		9				31		21		53
-9	-203	-181		-137	-115		-71	-49		-5	17		61	83		127	149		193	215	
-8	-89		-67		-45		-23		-1		21		43		65		87		109		131
-7	-153	-131	-109	-87	-65	-43		1	23	45	67	89	111		155	177	199	221	243	265	
-6	-2				-5		1				23		17				7		67		
-5	-103	-81	-59	-37		7	29	51	73		117	139	161	183		227	249	271	293		337
-4	-39		-17		5		27		49		71		93		115		137		159		181
-3	-53	-31		13	35		79	101		145	167		211	233		277	299		343	365	
-2	-7		1		15		13		37		3		59		35		81		23		103
-1	-3	19	41	63	85	107	129	151	173	195	217	239	261	283	305	327	349	371	393	415	437
0	11																				
1	47	69	91	113	135	157	179	201	223	245	267	289	311	333	355	377	399	421	443	465	487
2	9		29		5		51		31		73		21		95		53		117		8
3	97	119		163	185		229	251		295	317		361	383		427	449		493	515	
4	61		83		105		127		149		171		193		215		237		259		281
5	147	169	191	213		257	279	301	323		367	389	411	433		477	499	521	543		587
6	43				65		19				49		109				131		71		
7	197	219	241	263	285	307		351	373	395	417	439	461		505	527	549	571	593	615	
8	111		133		155		177		199		221		243		265		287		309		331
9	247	269		313	335		379	401		445	467		511	533		577	599		643	665	
10	17		79				101		7		123		67				39		167		89
11	297	319	341	363	385	407	429	451	473	495		539	561	583	605	627	649	671	693	715	737
12	161				205		227				271		293				337		359		
13	347	369	391	413	435	457	479	501	523	545	567	589		633	655	677	699	721	743	765	787
14	93		13		115				137		37		159		85		181		12		
15	397	419		463			529	551			617		661	683		727	749		793		
16	211		233		255		277		299		321		343		365		387		409		431
17	447	469	491	513	535	557	579	601	623	645	667	689	711	733	755	777		821	843	865	887

$q = 2^7$, $Va + Ub = 25a + 22b$

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
-17	-403	-381	-359	-337	-315	-293	-271	-249	-227	-205	-183	-161	-139	-117	-95	-73		-29	-7	15	37
-16	-189		-167		-145		-123		-101		-79		-57		-35		-13		9		31
-15	-353	-331		-287			-221	-199			-133		-89	-67		-23	-1		43		
-14	-41		-71		-15				-19		-27		-1		-5		3		17		
-13	-303	-281	-259	-237	-215	-193	-171	-149	-127	-105	-83	-61		-17	5	27	49	71	93	115	137
-12	-139				-95		-73				-29		-7				37		59		
-11	-253	-231	-209	-187	-165	-143	-121	-99	-77	-55		-11	11	33	55	77	99	121	143	165	187
-10	-57		-23				-3		-13		-1		9				31		21		53
-9	-203	-181		-137	-115		-71	-49		-5	17		61	83		127	149		193	215	
-8	-89		-67		-45		-23		-1		21		43		65		87		109		131
-7	-153	-131	-109	-87	-65	-43		1	23	45	67	89	111		155	177	199	221	243	265	
-6	-1				-5		1				23		17				7		67		
-5	-103	-81	-59	-37		7	29	51	73		117	139	161	183		227	249	271	293		337
-4	-39		-17		5		27		49		71		93		115		137		159		181
-3	-53	-31		13	35		79	101		145	167		211	233		277	299		343	365	
-2	-7		1		15		13		37		3		59		35		81		23		103
-1	-3	19	41	63	85	107	129	151	173	195	217	239	261	283	305	327	349	371	393	415	437
0	11																				
1	47	69	91	113	135	157	179	201	223	245	267	289	311	333	355	377	399	421	443	465	487
2	9		29		5		51		31		73		21		95		53		117		4
3	97	119		163	185		229	251		295	317		361	383		427	449		493	515	
4	61		83		105		127		149		171		193		215		237		259		281
5	147	169	191	213		257	279	301	323		367	389	411	433		477	499	521	543		587
6	43				65		19				49		109				131		71		
7	197	219	241	263	285	307		351	373	395	417	439	461		505	527	549	571	593	615	
8	111		133		155		177		199		221		243		265		287		309		331
9	247	269		313	335		379	401		445	467		511	533		577	599		643	665	
10	17		79				101		7		123		67				39		167		89
11	297	319	341	363	385	407	429	451	473	495		539	561	583	605	627	649	671	693	715	737
12	161				205		227				271		293				337		359		
13	347	369	391	413	435	457	479	501	523	545	567	589		633	655	677	699	721	743	765	787
14	93		13		115				137		37		159		85		181		6		
15	397	419		463			529	551			617		661	683		727	749		793		
16	211		233		255		277		299		321		343		365		387		409		431
17	447	469	491	513	535	557	579	601	623	645	667	689	711	733	755	777		821	843	865	887

$q = 2^8$, $Va + Ub = 25a + 22b$

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
-17	-403	-381	-359	-337	-315	-293	-271	-249	-227	-205	-183	-161	-139	-117	-95	-73		-29	-7	15	37
-16	-189		-167		-145		-123		-101		-79		-57		-35		-13		9		31
-15	-353	-331		-287			-221	-199			-133		-89	-67		-23	-1		43		
-14	-41		-71		-15				-19		-27		-1		-5		3		17		
-13	-303	-281	-259	-237	-215	-193	-171	-149	-127	-105	-83	-61		-17	5	27	49	71	93	115	137
-12	-139				-95		-73				-29		-7				37		59		
-11	-253	-231	-209	-187	-165	-143	-121	-99	-77	-55		-11	11	33	55	77	99	121	143	165	187
-10	-57		-23				-3		-13		-1		9				31		21		53
-9	-203	-181		-137	-115		-71	-49		-5	17		61	83		127	149		193	215	
-8	-89		-67		-45		-23		-1		21		43		65		87		109		131
-7	-153	-131	-109	-87	-65	-43		1	23	45	67	89	111		155	177	199	221	243	265	
-6	-1				-5		1				23		17				7		67		
-5	-103	-81	-59	-37		7	29	51	73		117	139	161	183		227	249	271	293		337
-4	-39		-17		5		27		49		71		93		115		137		159		181
-3	-53	-31		13	35		79	101		145	167		211	233		277	299		343	365	
-2	-7		1		15		13		37		3		59		35		81		23		103
-1	-3	19	41	63	85	107	129	151	173	195	217	239	261	283	305	327	349	371	393	415	437
0	11																				
1	47	69	91	113	135	157	179	201	223	245	267	289	311	333	355	377	399	421	443	465	487
2	9		29		5		51		31		73		21		95		53		117		4
3	97	119		163	185		229	251		295	317		361	383		427	449		493	515	
4	61		83		105		127		149		171		193		215		237		259		281
5	147	169	191	213		257	279	301	323		367	389	411	433		477	499	521	543		587
6	43				65		19				49		109				131		71		
7	197	219	241	263	285	307		351	373	395	417	439	461		505	527	549	571	593	615	
8	111		133		155		177		199		221		243		265		287		309		331
9	247	269		313	335		379	401		445	467		511	533		577	599		643	665	
10	17		79				101		7		123		67				39		167		89
11	297	319	341	363	385	407	429	451	473	495		539	561	583	605	627	649	671	693	715	737
12	161				205		227				271		293				337		359		
13	347	369	391	413	435	457	479	501	523	545	567	589		633	655	677	699	721	743	765	787
14	93		13		115				137		37		159		85		181		6		
15	397	419		463			529	551			617		661	683		727	749		793		
16	211		233		255		277		299		321		343		365		387		409		431
17	447	469	491	513	535	557	579	601	623	645	667	689	711	733	755	777		821	843	865	887

$q = 2^8$, $Va + Ub = 25a + 22b$

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
-17	-403	-381	-359	-337	-315	-293	-271	-249	-227	-205	-183	-161	-139	-117	-95	-73		-29	-7	15	37
-16	-189		-167		-145		-123		-101		-79		-57		-35		-13		9		31
-15	-353	-331		-287			-221	-199			-133		-89	-67		-23	-1		43		
-14	-41		-71		-15				-19		-27		-1		-5		3		17		
-13	-303	-281	-259	-237	-215	-193	-171	-149	-127	-105	-83	-61		-17	5	27	49	71	93	115	137
-12	-139				-95		-73				-29		-7				37		59		
-11	-253	-231	-209	-187	-165	-143	-121	-99	-77	-55		-11	11	33	55	77	99	121	143	165	187
-10	-57		-23				-3		-13		-1		9				31		21		53
-9	-203	-181		-137	-115		-71	-49		-5	17		61	83		127	149		193	215	
-8	-89		-67		-45		-23		-1		21		43		65		87		109		131
-7	-153	-131	-109	-87	-65	-43		1	23	45	67	89	111		155	177	199	221	243	265	
-6	-1				-5		1				23		17				7		67		
-5	-103	-81	-59	-37		7	29	51	73		117	139	161	183		227	249	271	293		337
-4	-39		-17		5		27		49		71		93		115		137		159		181
-3	-53	-31		13	35		79	101		145	167		211	233		277	299		343	365	
-2	-7		1		15		13		37		3		59		35		81		23		103
-1	-3	19	41	63	85	107	129	151	173	195	217	239	261	283	305	327	349	371	393	415	437
0	11																				
1	47	69	91	113	135	157	179	201	223	245	267	289	311	333	355	377	399	421	443	465	487
2	9		29		5		51		31		73		21		95		53		117		2
3	97	119		163	185		229	251		295	317		361	383		427	449		493	515	
4	61		83		105		127		149		171		193		215		237		259		281
5	147	169	191	213		257	279	301	323		367	389	411	433		477	499	521	543		587
6	43				65		19				49		109				131		71		
7	197	219	241	263	285	307		351	373	395	417	439	461		505	527	549	571	593	615	
8	111		133		155		177		199		221		243		265		287		309		331
9	247	269		313	335		379	401		445	467		511	533		577	599		643	665	
10	17		79				101		7		123		67				39		167		89
11	297	319	341	363	385	407	429	451	473	495		539	561	583	605	627	649	671	693	715	737
12	161				205		227				271		293				337		359		
13	347	369	391	413	435	457	479	501	523	545	567	589		633	655	677	699	721	743	765	787
14	93		13		115				137		37		159		85		181		3		
15	397	419		463			529	551			617		661	683		727	749		793		
16	211		233		255		277		299		321		343		365		387		409		431
17	447	469	491	513	535	557	579	601	623	645	667	689	711	733	755	777		821	843	865	887

$q = 2^9$, $Va + Ub = 25a + 22b$

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
-17	-403	-381	-359	-337	-315	-293	-271	-249	-227	-205	-183	-161	-139	-117	-95	-73		-29	-7	15	37
-16	-189		-167		-145		-123		-101		-79		-57		-35		-13		9		31
-15	-353	-331		-287			-221	-199			-133		-89	-67		-23	-1		43		
-14	-41		-71		-15				-19		-27		-1		-5		3		17		
-13	-303	-281	-259	-237	-215	-193	-171	-149	-127	-105	-83	-61		-17	5	27	49	71	93	115	137
-12	-139				-95		-73				-29		-7				37		59		
-11	-253	-231	-209	-187	-165	-143	-121	-99	-77	-55		-11	11	33	55	77	99	121	143	165	187
-10	-57		-23				-3		-13		-1		9				31		21		53
-9	-203	-181		-137	-115		-71	-49		-5	17		61	83		127	149		193	215	
-8	-89		-67		-45		-23		-1		21		43		65		87		109		131
-7	-153	-131	-109	-87	-65	-43		1	23	45	67	89	111		155	177	199	221	243	265	
-6	-1				-5		1				23		17				7		67		
-5	-103	-81	-59	-37		7	29	51	73		117	139	161	183		227	249	271	293		337
-4	-39		-17		5		27		49		71		93		115		137		159		181
-3	-53	-31		13	35		79	101		145	167		211	233		277	299		343	365	
-2	-7		1		15		13		37		3		59		35		81		23		103
-1	-3	19	41	63	85	107	129	151	173	195	217	239	261	283	305	327	349	371	393	415	437
0	11																				
1	47	69	91	113	135	157	179	201	223	245	267	289	311	333	355	377	399	421	443	465	487
2	9		29		5		51		31		73		21		95		53		117		2
3	97	119		163	185		229	251		295	317		361	383		427	449		493	515	
4	61		83		105		127		149		171		193		215		237		259		281
5	147	169	191	213		257	279	301	323		367	389	411	433		477	499	521	543		587
6	43				65		19				49		109				131		71		
7	197	219	241	263	285	307		351	373	395	417	439	461		505	527	549	571	593	615	
8	111		133		155		177		199		221		243		265		287		309		331
9	247	269		313	335		379	401		445	467		511	533		577	599		643	665	
10	17		79				101		7		123		67				39		167		89
11	297	319	341	363	385	407	429	451	473	495		539	561	583	605	627	649	671	693	715	737
12	161				205		227				271		293				337		359		
13	347	369	391	413	435	457	479	501	523	545	567	589		633	655	677	699	721	743	765	787
14	93		13		115				137		37		159		85		181		3		
15	397	419		463			529	551			617		661	683		727	749		793		
16	211		233		255		277		299		321		343		365		387		409		431
17	447	469	491	513	535	557	579	601	623	645	667	689	711	733	755	777		821	843	865	887

$q = 2^9$, $Va + Ub = 25a + 22b$

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
-17	-403	-381	-359	-337	-315	-293	-271	-249	-227	-205	-183	-161	-139	-117	-95	-73		-29	-7	15	37
-16	-189		-167		-145		-123		-101		-79		-57		-35		-13		9		31
-15	-353	-331		-287			-221	-199			-133		-89	-67		-23	-1		43		
-14	-41		-71		-15				-19		-27		-1		-5		3		17		
-13	-303	-281	-259	-237	-215	-193	-171	-149	-127	-105	-83	-61		-17	5	27	49	71	93	115	137
-12	-139				-95		-73				-29		-7				37		59		
-11	-253	-231	-209	-187	-165	-143	-121	-99	-77	-55		-11	11	33	55	77	99	121	143	165	187
-10	-57		-23				-3		-13		-1		9				31		21		53
-9	-203	-181		-137	-115		-71	-49		-5	17		61	83		127	149		193	215	
-8	-89		-67		-45		-23		-1		21		43		65		87		109		131
-7	-153	-131	-109	-87	-65	-43		1	23	45	67	89	111		155	177	199	221	243	265	
-6	-1				-5		1				23		17				7		67		
-5	-103	-81	-59	-37		7	29	51	73		117	139	161	183		227	249	271	293		337
-4	-39		-17		5		27		49		71		93		115		137		159		181
-3	-53	-31		13	35		79	101		145	167		211	233		277	299		343	365	
-2	-7		1		15		13		37		3		59		35		81		23		103
-1	-3	19	41	63	85	107	129	151	173	195	217	239	261	283	305	327	349	371	393	415	437
0	11																				
1	47	69	91	113	135	157	179	201	223	245	267	289	311	333	355	377	399	421	443	465	487
2	9		29		5		51		31		73		21		95		53		117		1
3	97	119		163	185		229	251		295	317		361	383		427	449		493	515	
4	61		83		105		127		149		171		193		215		237		259		281
5	147	169	191	213		257	279	301	323		367	389	411	433		477	499	521	543		587
6	43				65		19				49		109				131		71		
7	197	219	241	263	285	307		351	373	395	417	439	461		505	527	549	571	593	615	
8	111		133		155		177		199		221		243		265		287		309		331
9	247	269		313	335		379	401		445	467		511	533		577	599		643	665	
10	17		79				101		7		123		67				39		167		89
11	297	319	341	363	385	407	429	451	473	495		539	561	583	605	627	649	671	693	715	737
12	161				205		227				271		293				337		359		
13	347	369	391	413	435	457	479	501	523	545	567	589		633	655	677	699	721	743	765	787
14	93		13		115				137		37		159		85		181		3		
15	397	419		463			529	551			617		661	683		727	749		793		
16	211		233		255		277		299		321		343		365		387		409		431
17	447	469	491	513	535	557	579	601	623	645	667	689	711	733	755	777		821	843	865	887

$q = 3$, $Va + Ub = 25a + 22b$

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
-17	-403	-381	-359	-337	-315	-293	-271	-249	-227	-205	-183	-161	-139	-117	-95	-73		-29	-7	15	37
-16	-189		-167		-145		-123		-101		-79		-57		-35		-13		9		31
-15	-353	-331		-287			-221	-199			-133		-89	-67		-23	-1		43		
-14	-41		-71		-15				-19		-27		-1		-5		3		17		
-13	-303	-281	-259	-237	-215	-193	-171	-149	-127	-105	-83	-61		-17	5	27	49	71	93	115	137
-12	-139				-95		-73				-29		-7				37		59		
-11	-253	-231	-209	-187	-165	-143	-121	-99	-77	-55		-11	11	33	55	77	99	121	143	165	187
-10	-57		-23				-3		-13		-1		9				31		21		53
-9	-203	-181		-137	-115		-71	-49		-5	17		61	83		127	149		193	215	
-8	-89		-67		-45		-23		-1		21		43		65		87		109		131
-7	-153	-131	-109	-87	-65	-43		1	23	45	67	89	111		155	177	199	221	243	265	
-6	-1				-5		1				23		17				7		67		
-5	-103	-81	-59	-37		7	29	51	73		117	139	161	183		227	249	271	293		337
-4	-39		-17		5		27		49		71		93		115		137		159		181
-3	-53	-31		13	35		79	101		145	167		211	233		277	299		343	365	
-2	-7		1		15		13		37		3		59		35		81		23		103
-1	-3	19	41	63	85	107	129	151	173	195	217	239	261	283	305	327	349	371	393	415	437
0	11																				
1	47	69	91	113	135	157	179	201	223	245	267	289	311	333	355	377	399	421	443	465	487
2	9		29		5		51		31		73		21		95		53		117		1
3	97	119		163	185		229	251		295	317		361	383		427	449		493	515	
4	61		83		105		127		149		171		193		215		237		259		281
5	147	169	191	213		257	279	301	323		367	389	411	433		477	499	521	543		587
6	43				65		19				49		109				131		71		
7	197	219	241	263	285	307		351	373	395	417	439	461		505	527	549	571	593	615	
8	111		133		155		177		199		221		243		265		287		309		331
9	247	269		313	335		379	401		445	467		511	533		577	599		643	665	
10	17		79				101		7		123		67				39		167		89
11	297	319	341	363	385	407	429	451	473	495		539	561	583	605	627	649	671	693	715	737
12	161				205		227				271		293				337		359		
13	347	369	391	413	435	457	479	501	523	545	567	589		633	655	677	699	721	743	765	787
14	93		13		115				137		37		159		85		181		3		
15	397	419		463			529	551			617		661	683		727	749		793		
16	211		233		255		277		299		321		343		365		387		409		431
17	447	469	491	513	535	557	579	601	623	645	667	689	711	733	755	777		821	843	865	887

$q = 3$, $Va + Ub = 25a + 22b$

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
-17	-403	-127	-359	-337	-105	-293	-271	-83	-227	-205	-61	-161	-139	-39	-95	-73		-29	-7	5	37
-16	-63		-167		-145		-41		-101		-79		-19		-35		-13		3		31
-15	-353	-331		-287			-221	-199			-133		-89	-67		-23	-1		43		
-14	-41		-71		-5				-19		-9		-1		-5		1		17		
-13	-101	-281	-259	-79	-215	-193	-57	-149	-127	-35	-83	-61		-17	5	9	49	71	31	115	137
-12	-139				-95		-73				-29		-7				37		59		
-11	-253	-77	-209	-187	-55	-143	-121	-33	-77	-55		-11	11	11	55	77	33	121	143	55	187
-10	-19		-23				-1		-13		-1		3				31		7		53
-9	-203	-181		-137	-115		-71	-49		-5	17		61	83		127	149		193	215	
-8	-89		-67		-15		-23		-1		7		43		65		29		109		131
-7	-51	-131	-109	-29	-65	-43		1	23	15	67	89	37		155	59	199	221	81	265	
-6	-1				-5		1				23		17				7		67		
-5	-103	-27	-59	-37		7	29	17	73		39	139	161	61		227	83	271	293		337
-4	-13		-17		5		9		49		71		31		115		137		53		181
-3	-53	-31		13	35		79	101		145	167		211	233		277	299		343	365	
-2	-7		1		5		13		37		1		59		35		27		23		103
-1	-1	19	41	21	85	107	43	151	173	65	217	239	87	283	305	109	349	371	131	415	437
0	11																				
1	47	23	91	113	45	157	179	67	223	245	89	289	311	111	355	377	133	421	443	155	487
2	3		29		5		17		31		73		7		95		53		39		1
3	97	119		163	185		229	251		295	317		361	383		427	449		493	515	
4	61		83		35		127		149		57		193		215		79		259		281
5	49	169	191	71		257	93	301	323		367	389	137	433		159	499	521	181		587
6	43				65		19				49		109				131		71		
7	197	73	241	263	95	307		117	373	395	139	439	461		505	527	183	571	593	205	
8	37		133		155		59		199		221		81		265		287		103		331
9	247	269		313	335		379	401		445	467		511	533		577	599		643	665	
10	17		79				101		7		41		67				13		167		89
11	99	319	341	121	385	407	143	451	473	165		539	187	583	605	209	649	671	231	715	737
12	161				205		227				271		293				337		359		
13	347	123	391	413	145	457	479	167	523	545	189	589		211	655	677	233	721	743	255	787
14	31		13		115				137		37		53		85		181		1		
15	397	419		463			529	551			617		661	683		727	749		793		
16	211		233		85		277		299		107		343		365		129		409		431
17	149	469	491	171	535	557	193	601	623	215	667	689	237	733	755	259		821	281	865	887

$q = 3^2$, $Va + Ub = 25a + 22b$

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
-17	-403	-127	-359	-337	-105	-293	-271	-83	-227	-205	-61	-161	-139	-39	-95	-73		-29	-7	5	37
-16	-63		-167		-145		-41		-101		-79		-19		-35		-13		3		31
-15	-353	-331		-287			-221	-199			-133		-89	-67		-23	-1		43		
-14	-41		-71		-5				-19		-9		-1		-5		1		17		
-13	-101	-281	-259	-79	-215	-193	-57	-149	-127	-35	-83	-61		-17	5	9	49	71	31	115	137
-12	-139				-95		-73				-29		-7				37		59		
-11	-253	-77	-209	-187	-55	-143	-121	-33	-77	-55		-11	11	11	55	77	33	121	143	55	187
-10	-19		-23				-1		-13		-1		3				31		7		53
-9	-203	-181		-137	-115		-71	-49		-5	17		61	83		127	149		193	215	
-8	-89		-67		-15		-23		-1		7		43		65		29		109		131
-7	-51	-131	-109	-29	-65	-43		1	23	15	67	89	37		155	59	199	221	81	265	
-6	-1				-5		1				23		17				7		67		
-5	-103	-27	-59	-37		7	29	17	73		39	139	161	61		227	83	271	293		337
-4	-13		-17		5		9		49		71		31		115		137		53		181
-3	-53	-31		13	35		79	101		145	167		211	233		277	299		343	365	
-2	-7		1		5		13		37		1		59		35		27		23		103
-1	-1	19	41	21	85	107	43	151	173	65	217	239	87	283	305	109	349	371	131	415	437
0	11																				
1	47	23	91	113	45	157	179	67	223	245	89	289	311	111	355	377	133	421	443	155	487
2	3		29		5		17		31		73		7		95		53		39		1
3	97	119		163	185		229	251		295	317		361	383		427	449		493	515	
4	61		83		35		127		149		57		193		215		79		259		281
5	49	169	191	71		257	93	301	323		367	389	137	433		159	499	521	181		587
6	43				65		19				49		109				131		71		
7	197	73	241	263	95	307		117	373	395	139	439	461		505	527	183	571	593	205	
8	37		133		155		59		199		221		81		265		287		103		331
9	247	269		313	335		379	401		445	467		511	533		577	599		643	665	
10	17		79				101		7		41		67				13		167		89
11	99	319	341	121	385	407	143	451	473	165		539	187	583	605	209	649	671	231	715	737
12	161				205		227				271		293				337		359		
13	347	123	391	413	145	457	479	167	523	545	189	589		211	655	677	233	721	743	255	787
14	31		13		115				137		37		53		85		181		1		
15	397	419		463			529	551			617		661	683		727	749		793		
16	211		233		85		277		299		107		343		365		129		409		431
17	149	469	491	171	535	557	193	601	623	215	667	689	237	733	755	259		821	281	865	887

$q = 3^2$, $Va + Ub = 25a + 22b$

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
-17	-403	-127	-359	-337	-35	-293	-271	-83	-227	-205	-61	-161	-139	-13	-95	-73		-29	-7	5	37
-16	-21		-167		-145		-41		-101		-79		-19		-35		-13		1		31
-15	-353	-331		-287			-221	-199			-133		-89	-67		-23	-1		43		
-14	-41		-71		-5				-19		-3		-1		-5		1		17		
-13	-101	-281	-259	-79	-215	-193	-19	-149	-127	-35	-83	-61		-17	5	3	49	71	31	115	137
-12	-139				-95		-73				-29		-7				37		59		
-11	-253	-77	-209	-187	-55	-143	-121	-11	-77	-55		-11	11	11	55	77	11	121	143	55	187
-10	-19		-23				-1		-13		-1		1				31		7		53
-9	-203	-181		-137	-115		-71	-49		-5	17		61	83		127	149		193	215	
-8	-89		-67		-5		-23		-1		7		43		65		29		109		131
-7	-17	-131	-109	-29	-65	-43		1	23	5	67	89	37		155	59	199	221	27	265	
-6	-1				-5		1				23		17				7		67		
-5	-103	-9	-59	-37		7	29	17	73		13	139	161	61		227	83	271	293		337
-4	-13		-17		5		3		49		71		31		115		137		53		181
-3	-53	-31		13	35		79	101		145	167		211	233		277	299		343	365	
-2	-7		1		5		13		37		1		59		35		9		23		103
-1	-1	19	41	7	85	107	43	151	173	65	217	239	29	283	305	109	349	371	131	415	437
0	11																				
1	47	23	91	113	15	157	179	67	223	245	89	289	311	37	355	377	133	421	443	155	487
2	1		29		5		17		31		73		7		95		53		13		1
3	97	119		163	185		229	251		295	317		361	383		427	449		493	515	
4	61		83		35		127		149		19		193		215		79		259		281
5	49	169	191	71		257	31	301	323		367	389	137	433		53	499	521	181		587
6	43				65		19				49		109				131		71		
7	197	73	241	263	95	307		39	373	395	139	439	461		505	527	61	571	593	205	
8	37		133		155		59		199		221		27		265		287		103		331
9	247	269		313	335		379	401		445	467		511	533		577	599		643	665	
10	17		79				101		7		41		67				13		167		89
11	33	319	341	121	385	407	143	451	473	55		539	187	583	605	209	649	671	77	715	737
12	161				205		227				271		293				337		359		
13	347	41	391	413	145	457	479	167	523	545	63	589		211	655	677	233	721	743	85	787
14	31		13		115				137		37		53		85		181		1		
15	397	419		463			529	551			617		661	683		727	749		793		
16	211		233		85		277		299		107		343		365		43		409		431
17	149	469	491	57	535	557	193	601	623	215	667	689	79	733	755	259		821	281	865	887

$q = 3^3$, $Va + Ub = 25a + 22b$

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
-17	-403	-127	-359	-337	-35	-293	-271	-83	-227	-205	-61	-161	-139	-13	-95	-73		-29	-7	5	37
-16	-21		-167		-145		-41		-101		-79		-19		-35		-13		1		31
-15	-353	-331		-287			-221	-199			-133		-89	-67		-23	-1		43		
-14	-41		-71		-5				-19		-3		-1		-5		1		17		
-13	-101	-281	-259	-79	-215	-193	-19	-149	-127	-35	-83	-61		-17	5	3	49	71	31	115	137
-12	-139				-95		-73				-29		-7				37		59		
-11	-253	-77	-209	-187	-55	-143	-121	-11	-77	-55		-11	11	11	55	77	11	121	143	55	187
-10	-19		-23				-1		-13		-1		1				31		7		53
-9	-203	-181		-137	-115		-71	-49		-5	17		61	83		127	149		193	215	
-8	-89		-67		-5		-23		-1		7		43		65		29		109		131
-7	-17	-131	-109	-29	-65	-43		1	23	5	67	89	37		155	59	199	221	27	265	
-6	-1				-5		1				23		17				7		67		
-5	-103	-9	-59	-37		7	29	17	73		13	139	161	61		227	83	271	293		337
-4	-13		-17		5		3		49		71		31		115		137		53		181
-3	-53	-31		13	35		79	101		145	167		211	233		277	299		343	365	
-2	-7		1		5		13		37		1		59		35		9		23		103
-1	-1	19	41	7	85	107	43	151	173	65	217	239	29	283	305	109	349	371	131	415	437
0	11																				
1	47	23	91	113	15	157	179	67	223	245	89	289	311	37	355	377	133	421	443	155	487
2	1		29		5		17		31		73		7		95		53		13		1
3	97	119		163	185		229	251		295	317		361	383		427	449		493	515	
4	61		83		35		127		149		19		193		215		79		259		281
5	49	169	191	71		257	31	301	323		367	389	137	433		53	499	521	181		587
6	43				65		19				49		109				131		71		
7	197	73	241	263	95	307		39	373	395	139	439	461		505	527	61	571	593	205	
8	37		133		155		59		199		221		27		265		287		103		331
9	247	269		313	335		379	401		445	467		511	533		577	599		643	665	
10	17		79				101		7		41		67				13		167		89
11	33	319	341	121	385	407	143	451	473	55		539	187	583	605	209	649	671	77	715	737
12	161				205		227				271		293				337		359		
13	347	41	391	413	145	457	479	167	523	545	63	589		211	655	677	233	721	743	85	787
14	31		13		115				137		37		53		85		181		1		
15	397	419		463			529	551			617		661	683		727	749		793		
16	211		233		85		277		299		107		343		365		43		409		431
17	149	469	491	57	535	557	193	601	623	215	667	689	79	733	755	259		821	281	865	887

$q = 3^3$, $Va + Ub = 25a + 22b$

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
-17	-403	-127	-359	-337	-35	-293	-271	-83	-227	-205	-61	-161	-139	-13	-95	-73		-29	-7	5	37
-16	-7		-167		-145		-41		-101		-79		-19		-35		-13		1		31
-15	-353	-331		-287			-221	-199			-133		-89	-67		-23	-1		43		
-14	-41		-71		-5				-19		-1		-1		-5		1		17		
-13	-101	-281	-259	-79	-215	-193	-19	-149	-127	-35	-83	-61		-17	5	1	49	71	31	115	137
-12	-139				-95		-73				-29		-7				37		59		
-11	-253	-77	-209	-187	-55	-143	-121	-11	-77	-55		-11	11	11	55	77	11	121	143	55	187
-10	-19		-23				-1		-13		-1		1				31		7		53
-9	-203	-181		-137	-115		-71	-49		-5	17		61	83		127	149		193	215	
-8	-89		-67		-5		-23		-1		7		43		65		29		109		131
-7	-17	-131	-109	-29	-65	-43		1	23	5	67	89	37		155	59	199	221	9	265	
-6	-1				-5		1				23		17				7		67		
-5	-103	-3	-59	-37		7	29	17	73		13	139	161	61		227	83	271	293		337
-4	-13		-17		5		1		49		71		31		115		137		53		181
-3	-53	-31		13	35		79	101		145	167		211	233		277	299		343	365	
-2	-7		1		5		13		37		1		59		35		3		23		103
-1	-1	19	41	7	85	107	43	151	173	65	217	239	29	283	305	109	349	371	131	415	437
0	11																				
1	47	23	91	113	5	157	179	67	223	245	89	289	311	37	355	377	133	421	443	155	487
2	1		29		5		17		31		73		7		95		53		13		1
3	97	119		163	185		229	251		295	317		361	383		427	449		493	515	
4	61		83		35		127		149		19		193		215		79		259		281
5	49	169	191	71		257	31	301	323		367	389	137	433		53	499	521	181		587
6	43				65		19				49		109				131		71		
7	197	73	241	263	95	307		13	373	395	139	439	461		505	527	61	571	593	205	
8	37		133		155		59		199		221		9		265		287		103		331
9	247	269		313	335		379	401		445	467		511	533		577	599		643	665	
10	17		79				101		7		41		67				13		167		89
11	11	319	341	121	385	407	143	451	473	55		539	187	583	605	209	649	671	77	715	737
12	161				205		227				271		293				337		359		
13	347	41	391	413	145	457	479	167	523	545	21	589		211	655	677	233	721	743	85	787
14	31		13		115				137		37		53		85		181		1		
15	397	419		463			529	551			617		661	683		727	749		793		
16	211		233		85		277		299		107		343		365		43		409		431
17	149	469	491	19	535	557	193	601	623	215	667	689	79	733	755	259		821	281	865	887

$q = 3^4,\ Va + Ub = 25a + 22b$

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
-17	-403	-127	-359	-337	-35	-293	-271	-83	-227	-205	-61	-161	-139	-13	-95	-73		-29	-7	5	37
-16	-7		-167		-145		-41		-101		-79		-19		-35		-13		1		31
-15	-353	-331		-287			-221	-199			-133		-89	-67		-23	-1		43		
-14	-41		-71		-5				-19		-1		-1		-5		1		17		
-13	-101	-281	-259	-79	-215	-193	-19	-149	-127	-35	-83	-61		-17	5	1	49	71	31	115	137
-12	-139				-95		-73				-29		-7				37		59		
-11	-253	-77	-209	-187	-55	-143	-121	-11	-77	-55		-11	11	11	55	77	11	121	143	55	187
-10	-19		-23				-1		-13		-1		1				31		7		53
-9	-203	-181		-137	-115		-71	-49		-5	17		61	83		127	149		193	215	
-8	-89		-67		-5		-23		-1		7		43		65		29		109		131
-7	-17	-131	-109	-29	-65	-43		1	23	5	67	89	37		155	59	199	221	9	265	
-6	-1				-5		1				23		17				7		67		
-5	-103	-3	-59	-37		7	29	17	73		13	139	161	61		227	83	271	293		337
-4	-13		-17		5		1		49		71		31		115		137		53		181
-3	-53	-31		13	35		79	101		145	167		211	233		277	299		343	365	
-2	-7		1		5		13		37		1		59		35		3		23		103
-1	-1	19	41	7	85	107	43	151	173	65	217	239	29	283	305	109	349	371	131	415	437
0	11																				
1	47	23	91	113	5	157	179	67	223	245	89	289	311	37	355	377	133	421	443	155	487
2	1		29		5		17		31		73		7		95		53		13		1
3	97	119		163	185		229	251		295	317		361	383		427	449		493	515	
4	61		83		35		127		149		19		193		215		79		259		281
5	49	169	191	71		257	31	301	323		367	389	137	433		53	499	521	181		587
6	43				65		19				49		109				131		71		
7	197	73	241	263	95	307		13	373	395	139	439	461		505	527	61	571	593	205	
8	37		133		155		59		199		221		9		265		287		103		331
9	247	269		313	335		379	401		445	467		511	533		577	599		643	665	
10	17		79				101		7		41		67				13		167		89
11	11	319	341	121	385	407	143	451	473	55		539	187	583	605	209	649	671	77	715	737
12	161				205		227				271		293				337		359		
13	347	41	391	413	145	457	479	167	523	545	21	589		211	655	677	233	721	743	85	787
14	31		13		115				137		37		53		85		181		1		
15	397	419		463			529	551			617		661	683		727	749		793		
16	211		233		85		277		299		107		343		365		43		409		431
17	149	469	491	19	535	557	193	601	623	215	667	689	79	733	755	259		821	281	865	887

$q = 3^4$, $Va + Ub = 25a + 22b$

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
-17	-403	-127	-359	-337	-35	-293	-271	-83	-227	-205	-61	-161	-139	-13	-95	-73		-29	-7	5	37
-16	-7		-167		-145		-41		-101		-79		-19		-35		-13		1		31
-15	-353	-331		-287			-221	-199			-133		-89	-67		-23	-1		43		
-14	-41		-71		-5				-19		-1		-1		-5		1		17		
-13	-101	-281	-259	-79	-215	-193	-19	-149	-127	-35	-83	-61		-17	5	1	49	71	31	115	137
-12	-139				-95		-73				-29		-7				37		59		
-11	-253	-77	-209	-187	-55	-143	-121	-11	-77	-55		-11	11	11	55	77	11	121	143	55	187
-10	-19		-23				-1		-13		-1		1				31		7		53
-9	-203	-181		-137	-115		-71	-49		-5	17		61	83		127	149		193	215	
-8	-89		-67		-5		-23		-1		7		43		65		29		109		131
-7	-17	-131	-109	-29	-65	-43		1	23	5	67	89	37		155	59	199	221	3	265	
-6	-1				-5		1				23		17				7		67		
-5	-103	-1	-59	-37		7	29	17	73		13	139	161	61		227	83	271	293		337
-4	-13		-17		5		1		49		71		31		115		137		53		181
-3	-53	-31		13	35		79	101		145	167		211	233		277	299		343	365	
-2	-7		1		5		13		37		1		59		35		1		23		103
-1	-1	19	41	7	85	107	43	151	173	65	217	239	29	283	305	109	349	371	131	415	437
0	11																				
1	47	23	91	113	5	157	179	67	223	245	89	289	311	37	355	377	133	421	443	155	487
2	1		29		5		17		31		73		7		95		53		13		1
3	97	119		163	185		229	251		295	317		361	383		427	449		493	515	
4	61		83		35		127		149		19		193		215		79		259		281
5	49	169	191	71		257	31	301	323		367	389	137	433		53	499	521	181		587
6	43				65		19				49		109				131		71		
7	197	73	241	263	95	307		13	373	395	139	439	461		505	527	61	571	593	205	
8	37		133		155		59		199		221		3		265		287		103		331
9	247	269		313	335		379	401		445	467		511	533		577	599		643	665	
10	17		79				101		7		41		67				13		167		89
11	11	319	341	121	385	407	143	451	473	55		539	187	583	605	209	649	671	77	715	737
12	161				205		227				271		293				337		359		
13	347	41	391	413	145	457	479	167	523	545	7	589		211	655	677	233	721	743	85	787
14	31		13		115				137		37		53		85		181		1		
15	397	419		463			529	551			617		661	683		727	749		793		
16	211		233		85		277		299		107		343		365		43		409		431
17	149	469	491	19	535	557	193	601	623	215	667	689	79	733	755	259		821	281	865	887

$q = 3^5$, $Va + Ub = 25a + 22b$

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
-17	-403	-127	-359	-337	-35	-293	-271	-83	-227	-205	-61	-161	-139	-13	-95	-73		-29	-7	5	37
-16	-7		-167		-145		-41		-101		-79		-19		-35		-13		1		31
-15	-353	-331		-287			-221	-199			-133		-89	-67		-23	-1		43		
-14	-41		-71		-5				-19		-1		-1		-5		1		17		
-13	-101	-281	-259	-79	-215	-193	-19	-149	-127	-35	-83	-61		-17	5	1	49	71	31	115	137
-12	-139				-95		-73				-29		-7				37		59		
-11	-253	-77	-209	-187	-55	-143	-121	-11	-77	-55		-11	11	11	55	77	11	121	143	55	187
-10	-19		-23				-1		-13		-1		1				31		7		53
-9	-203	-181		-137	-115		-71	-49		-5	17		61	83		127	149		193	215	
-8	-89		-67		-5		-23		-1		7		43		65		29		109		131
-7	-17	-131	-109	-29	-65	-43		1	23	5	67	89	37		155	59	199	221	3	265	
-6	-1				-5		1				23		17				7		67		
-5	-103	-1	-59	-37		7	29	17	73		13	139	161	61		227	83	271	293		337
-4	-13		-17		5		1		49		71		31		115		137		53		181
-3	-53	-31		13	35		79	101		145	167		211	233		277	299		343	365	
-2	-7		1		5		13		37		1		59		35		1		23		103
-1	-1	19	41	7	85	107	43	151	173	65	217	239	29	283	305	109	349	371	131	415	437
0	11																				
1	47	23	91	113	5	157	179	67	223	245	89	289	311	37	355	377	133	421	443	155	487
2	1		29		5		17		31		73		7		95		53		13		1
3	97	119		163	185		229	251		295	317		361	383		427	449		493	515	
4	61		83		35		127		149		19		193		215		79		259		281
5	49	169	191	71		257	31	301	323		367	389	137	433		53	499	521	181		587
6	43				65		19				49		109				131		71		
7	197	73	241	263	95	307		13	373	395	139	439	461		505	527	61	571	593	205	
8	37		133		155		59		199		221		3		265		287		103		331
9	247	269		313	335		379	401		445	467		511	533		577	599		643	665	
10	17		79				101		7		41		67				13		167		89
11	11	319	341	121	385	407	143	451	473	55		539	187	583	605	209	649	671	77	715	737
12	161				205		227				271		293				337		359		
13	347	41	391	413	145	457	479	167	523	545	7	589		211	655	677	233	721	743	85	787
14	31		13		115				137		37		53		85		181		1		
15	397	419		463			529	551			617		661	683		727	749		793		
16	211		233		85		277		299		107		343		365		43		409		431
17	149	469	491	19	535	557	193	601	623	215	667	689	79	733	755	259		821	281	865	887

$q = 3^5$, $Va + Ub = 25a + 22b$

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
-17	-403	-127	-359	-337	-35	-293	-271	-83	-227	-205	-61	-161	-139	-13	-95	-73		-29	-7	5	37
-16	-7		-167		-145		-41		-101		-79		-19		-35		-13		1		31
-15	-353	-331		-287			-221	-199			-133		-89	-67		-23	-1		43		
-14	-41		-71		-5				-19		-1		-1		-5		1		17		
-13	-101	-281	-259	-79	-215	-193	-19	-149	-127	-35	-83	-61		-17	5	1	49	71	31	115	137
-12	-139				-95		-73				-29		-7				37		59		
-11	-253	-77	-209	-187	-55	-143	-121	-11	-77	-55		-11	11	11	55	77	11	121	143	55	187
-10	-19		-23				-1		-13		-1		1				31		7		53
-9	-203	-181		-137	-115		-71	-49		-5	17		61	83		127	149		193	215	
-8	-89		-67		-5		-23		-1		7		43		65		29		109		131
-7	-17	-131	-109	-29	-65	-43		1	23	5	67	89	37		155	59	199	221	1	265	
-6	-1				-5		1				23		17				7		67		
-5	-103	-1	-59	-37		7	29	17	73		13	139	161	61		227	83	271	293		337
-4	-13		-17		5		1		49		71		31		115		137		53		181
-3	-53	-31		13	35		79	101		145	167		211	233		277	299		343	365	
-2	-7		1		5		13		37		1		59		35		1		23		103
-1	-1	19	41	7	85	107	43	151	173	65	217	239	29	283	305	109	349	371	131	415	437
0	11																				
1	47	23	91	113	5	157	179	67	223	245	89	289	311	37	355	377	133	421	443	155	487
2	1		29		5		17		31		73		7		95		53		13		1
3	97	119		163	185		229	251		295	317		361	383		427	449		493	515	
4	61		83		35		127		149		19		193		215		79		259		281
5	49	169	191	71		257	31	301	323		367	389	137	433		53	499	521	181		587
6	43				65		19				49		109				131		71		
7	197	73	241	263	95	307		13	373	395	139	439	461		505	527	61	571	593	205	
8	37		133		155		59		199		221		1		265		287		103		331
9	247	269		313	335		379	401		445	467		511	533		577	599		643	665	
10	17		79				101		7		41		67				13		167		89
11	11	319	341	121	385	407	143	451	473	55		539	187	583	605	209	649	671	77	715	737
12	161				205		227				271		293				337		359		
13	347	41	391	413	145	457	479	167	523	545	7	589		211	655	677	233	721	743	85	787
14	31		13		115				137		37		53		85		181		1		
15	397	419		463			529	551			617		661	683		727	749		793		
16	211		233		85		277		299		107		343		365		43		409		431
17	149	469	491	19	535	557	193	601	623	215	667	689	79	733	755	259		821	281	865	887

$q = 5$, $Va + Ub = 25a + 22b$

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
-17	-403	-127	-359	-337	-35	-293	-271	-83	-227	-205	-61	-161	-139	-13	-95	-73		-29	-7	5	37
-16	-7		-167		-145		-41		-101		-79		-19		-35		-13		1		31
-15	-353	-331		-287			-221	-199			-133		-89	-67		-23	-1		43		
-14	-41		-71		-5				-19		-1		-1		-5		1		17		
-13	-101	-281	-259	-79	-215	-193	-19	-149	-127	-35	-83	-61		-17	5	1	49	71	31	115	137
-12	-139				-95		-73				-29		-7				37		59		
-11	-253	-77	-209	-187	-55	-143	-121	-11	-77	-55		-11	11	11	55	77	11	121	143	55	187
-10	-19		-23				-1		-13		-1		1				31		7		53
-9	-203	-181		-137	-115		-71	-49		-5	17		61	83		127	149		193	215	
-8	-89		-67		-5		-23		-1		7		43		65		29		109		131
-7	-17	-131	-109	-29	-65	-43		1	23	5	67	89	37		155	59	199	221	1	265	
-6	-1				-5		1				23		17				7		67		
-5	-103	-1	-59	-37		7	29	17	73		13	139	161	61		227	83	271	293		337
-4	-13		-17		5		1		49		71		31		115		137		53		181
-3	-53	-31		13	35		79	101		145	167		211	233		277	299		343	365	
-2	-7		1		5		13		37		1		59		35		1		23		103
-1	-1	19	41	7	85	107	43	151	173	65	217	239	29	283	305	109	349	371	131	415	437
0	11																				
1	47	23	91	113	5	157	179	67	223	245	89	289	311	37	355	377	133	421	443	155	487
2	1		29		5		17		31		73		7		95		53		13		1
3	97	119		163	185		229	251		295	317		361	383		427	449		493	515	
4	61		83		35		127		149		19		193		215		79		259		281
5	49	169	191	71		257	31	301	323		367	389	137	433		53	499	521	181		587
6	43				65		19				49		109				131		71		
7	197	73	241	263	95	307		13	373	395	139	439	461		505	527	61	571	593	205	
8	37		133		155		59		199		221		1		265		287		103		331
9	247	269		313	335		379	401		445	467		511	533		577	599		643	665	
10	17		79				101		7		41		67				13		167		89
11	11	319	341	121	385	407	143	451	473	55		539	187	583	605	209	649	671	77	715	737
12	161				205		227				271		293				337		359		
13	347	41	391	413	145	457	479	167	523	545	7	589		211	655	677	233	721	743	85	787
14	31		13		115				137		37		53		85		181		1		
15	397	419		463			529	551			617		661	683		727	749		793		
16	211		233		85		277		299		107		343		365		43		409		431
17	149	469	491	19	535	557	193	601	623	215	667	689	79	733	755	259		821	281	865	887

$q = 5$, $Va + Ub = 25a + 22b$

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
-17	-403	-127	-359	-337	-7	-293	-271	-83	-227	-41	-61	-161	-139	-13	-19	-73		-29	-7	1	37
-16	-7		-167		-29		-41		-101		-79		-19		-7		-13		1		31
-15	-353	-331		-287			-221	-199			-133		-89	-67		-23	-1		43		
-14	-41		-71		-1				-19		-1		-1		-1		1		17		
-13	-101	-281	-259	-79	-43	-193	-19	-149	-127	-7	-83	-61		-17	1	1	49	71	31	23	137
-12	-139				-19		-73				-29		-7				37		59		
-11	-253	-77	-209	-187	-11	-143	-121	-11	-77	-11		-11	11	11	11	77	11	121	143	11	187
-10	-19		-23				-1		-13		-1		1				31		7		53
-9	-203	-181		-137	-23		-71	-49		-1	17		61	83		127	149		193	43	
-8	-89		-67		-1		-23		-1		7		43		13		29		109		131
-7	-17	-131	-109	-29	-13	-43		1	23	1	67	89	37		31	59	199	221	1	53	
-6	-1				-1		1				23		17				7		67		
-5	-103	-1	-59	-37		7	29	17	73		13	139	161	61		227	83	271	293		337
-4	-13		-17		1		1		49		71		31		23		137		53		181
-3	-53	-31		13	7		79	101		29	167		211	233		277	299		343	73	
-2	-7		1		1		13		37		1		59		7		1		23		103
-1	-1	19	41	7	17	107	43	151	173	13	217	239	29	283	61	109	349	371	131	83	437
0	11																				
1	47	23	91	113	1	157	179	67	223	49	89	289	311	37	71	377	133	421	443	31	487
2	1		29		1		17		31		73		7		19		53		13		1
3	97	119		163	37		229	251		59	317		361	383		427	449		493	103	
4	61		83		7		127		149		19		193		43		79		259		281
5	49	169	191	71		257	31	301	323		367	389	137	433		53	499	521	181		587
6	43				13		19				49		109				131		71		
7	197	73	241	263	19	307		13	373	79	139	439	461		101	527	61	571	593	41	
8	37		133		31		59		199		221		1		53		287		103		331
9	247	269		313	67		379	401		89	467		511	533		577	599		643	133	
10	17		79				101		7		41		67				13		167		89
11	11	319	341	121	77	407	143	451	473	11		539	187	583	121	209	649	671	77	143	737
12	161				41		227				271		293				337		359		
13	347	41	391	413	29	457	479	167	523	109	7	589		211	131	677	233	721	743	17	787
14	31		13		23				137		37		53		17		181		1		
15	397	419		463			529	551			617		661	683		727	749		793		
16	211		233		17		277		299		107		343		73		43		409		431
17	149	469	491	19	107	557	193	601	623	43	667	689	79	733	151	259		821	281	173	887

$q = 7$, $Va + Ub = 25a + 22b$

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
-17	-403	-127	-359	-337	-7	-293	-271	-83	-227	-41	-61	-161	-139	-13	-19	-73		-29	-7	1	37
-16	-7		-167		-29		-41		-101		-79		-19		-7		-13		1		31
-15	-353	-331		-287			-221	-199			-133		-89	-67		-23	-1		43		
-14	-41		-71		-1				-19		-1		-1		-1		1		17		
-13	-101	-281	-259	-79	-43	-193	-19	-149	-127	-7	-83	-61		-17	1	1	49	71	31	23	137
-12	-139				-19		-73				-29		-7				37		59		
-11	-253	-77	-209	-187	-11	-143	-121	-11	-77	-11		-11	11	11	11	77	11	121	143	11	187
-10	-19		-23				-1		-13		-1		1				31		7		53
-9	-203	-181		-137	-23		-71	-49		-1	17		61	83		127	149		193	43	
-8	-89		-67		-1		-23		-1		7		43		13		29		109		131
-7	-17	-131	-109	-29	-13	-43		1	23	1	67	89	37		31	59	199	221	1	53	
-6	-1				-1		1				23		17				7		67		
-5	-103	-1	-59	-37		7	29	17	73		13	139	161	61		227	83	271	293		337
-4	-13		-17		1		1		49		71		31		23		137		53		181
-3	-53	-31		13	7		79	101		29	167		211	233		277	299		343	73	
-2	-7		1		1		13		37		1		59		7		1		23		103
-1	-1	19	41	7	17	107	43	151	173	13	217	239	29	283	61	109	349	371	131	83	437
0	11																				
1	47	23	91	113	1	157	179	67	223	49	89	289	311	37	71	377	133	421	443	31	487
2	1		29		1		17		31		73		7		19		53		13		1
3	97	119		163	37		229	251		59	317		361	383		427	449		493	103	
4	61		83		7		127		149		19		193		43		79		259		281
5	49	169	191	71		257	31	301	323		367	389	137	433		53	499	521	181		587
6	43				13		19				49		109				131		71		
7	197	73	241	263	19	307		13	373	79	139	439	461		101	527	61	571	593	41	
8	37		133		31		59		199		221		1		53		287		103		331
9	247	269		313	67		379	401		89	467		511	533		577	599		643	133	
10	17		79				101		7		41		67				13		167		89
11	11	319	341	121	77	407	143	451	473	11		539	187	583	121	209	649	671	77	143	737
12	161				41		227				271		293				337		359		
13	347	41	391	413	29	457	479	167	523	109	7	589		211	131	677	233	721	743	17	787
14	31		13		23				137		37		53		17		181		1		
15	397	419		463			529	551			617		661	683		727	749		793		
16	211		233		17		277		299		107		343		73		43		409		431
17	149	469	491	19	107	557	193	601	623	43	667	689	79	733	151	259		821	281	173	887

$q = 7$, $Va + Ub = 25a + 22b$

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
-17	-403	-127	-359	-337	-1	-293	-271	-83	-227	-41	-61	-23	-139	-13	-19	-73		-29	-1	1	37
-16	-1		-167		-29		-41		-101		-79		-19		-1		-13		1		31
-15	-353	-331		-41			-221	-199			-19		-89	-67		-23	-1		43		
-14	-41		-71		-1				-19		-1		-1		-1		1		17		
-13	-101	-281	-37	-79	-43	-193	-19	-149	-127	-1	-83	-61		-17	1	1	7	71	31	23	137
-12	-139				-19		-73				-29		-1				37		59		
-11	-253	-11	-209	-187	-11	-143	-121	-11	-11	-11		-11	11	11	11	11	11	121	143	11	187
-10	-19		-23				-1		-13		-1		1				31		1		53
-9	-29	-181		-137	-23		-71	-7		-1	17		61	83		127	149		193	43	
-8	-89		-67		-1		-23		-1		1		43		13		29		109		131
-7	-17	-131	-109	-29	-13	-43		1	23	1	67	89	37		31	59	199	221	1	53	
-6	-1				-1		1				23		17				1		67		
-5	-103	-1	-59	-37		1	29	17	73		13	139	23	61		227	83	271	293		337
-4	-13		-17		1		1		7		71		31		23		137		53		181
-3	-53	-31		13	1		79	101		29	167		211	233		277	299		49	73	
-2	-1		1		1		13		37		1		59		1		1		23		103
-1	-1	19	41	1	17	107	43	151	173	13	31	239	29	283	61	109	349	53	131	83	437
0	11																				
1	47	23	13	113	1	157	179	67	223	7	89	289	311	37	71	377	19	421	443	31	487
2	1		29		1		17		31		73		1		19		53		13		1
3	97	17		163	37		229	251		59	317		361	383		61	449		493	103	
4	61		83		1		127		149		19		193		43		79		37		281
5	7	169	191	71		257	31	43	323		367	389	137	433		53	499	521	181		587
6	43				13		19				7		109				131		71		
7	197	73	241	263	19	307		13	373	79	139	439	461		101	527	61	571	593	41	
8	37		19		31		59		199		221		1		53		41		103		331
9	247	269		313	67		379	401		89	467		73	533		577	599		643	19	
10	17		79				101		1		41		67				13		167		89
11	11	319	341	121	11	407	143	451	473	11		77	187	583	121	209	649	671	11	143	737
12	23				41		227				271		293				337		359		
13	347	41	391	59	29	457	479	167	523	109	1	589		211	131	677	233	103	743	17	787
14	31		13		23				137		37		53		17		181		1		
15	397	419		463			529	551			617		661	683		727	107		793		
16	211		233		17		277		299		107		49		73		43		409		431
17	149	67	491	19	107	557	193	601	89	43	667	689	79	733	151	37		821	281	173	887

$q = 7^2,\ Va + Ub = 25a + 22b$

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
-17	-403	-127	-359	-337	-1	-293	-271	-83	-227	-41	-61	-23	-139	-13	-19	-73		-29	-1	1	37
-16	-1		-167		-29		-41		-101		-79		-19		-1		-13		1		31
-15	-353	-331		-41			-221	-199			-19		-89	-67		-23	-1		43		
-14	-41		-71		-1				-19		-1		-1		-1		1		17		
-13	-101	-281	-37	-79	-43	-193	-19	-149	-127	-1	-83	-61		-17	1	1	7	71	31	23	137
-12	-139				-19		-73				-29		-1				37		59		
-11	-253	-11	-209	-187	-11	-143	-121	-11	-11	-11		-11	11	11	11	11	11	121	143	11	187
-10	-19		-23				-1		-13		-1		1				31		1		53
-9	-29	-181		-137	-23		-71	-7		-1	17		61	83		127	149		193	43	
-8	-89		-67		-1		-23		-1		1		43		13		29		109		131
-7	-17	-131	-109	-29	-13	-43		1	23	1	67	89	37		31	59	199	221	1	53	
-6	-1				-1		1				23		17				1		67		
-5	-103	-1	-59	-37		1	29	17	73		13	139	23	61		227	83	271	293		337
-4	-13		-17		1		1		7		71		31		23		137		53		181
-3	-53	-31		13	1		79	101		29	167		211	233		277	299		49	73	
-2	-1		1		1		13		37		1		59		1		1		23		103
-1	-1	19	41	1	17	107	43	151	173	13	31	239	29	283	61	109	349	53	131	83	437
0	11																				
1	47	23	13	113	1	157	179	67	223	7	89	289	311	37	71	377	19	421	443	31	487
2	1		29		1		17		31		73		1		19		53		13		1
3	97	17		163	37		229	251		59	317		361	383		61	449		493	103	
4	61		83		1		127		149		19		193		43		79		37		281
5	7	169	191	71		257	31	43	323		367	389	137	433		53	499	521	181		587
6	43				13		19				7		109				131		71		
7	197	73	241	263	19	307		13	373	79	139	439	461		101	527	61	571	593	41	
8	37		19		31		59		199		221		1		53		41		103		331
9	247	269		313	67		379	401		89	467		73	533		577	599		643	19	
10	17		79				101		1		41		67				13		167		89
11	11	319	341	121	11	407	143	451	473	11		77	187	583	121	209	649	671	11	143	737
12	23				41		227				271		293				337		359		
13	347	41	391	59	29	457	479	167	523	109	1	589		211	131	677	233	103	743	17	787
14	31		13		23				137		37		53		17		181		1		
15	397	419		463			529	551			617		661	683		727	107		793		
16	211		233		17		277		299		107		49		73		43		409		431
17	149	67	491	19	107	557	193	601	89	43	667	689	79	733	151	37		821	281	173	887

$q = 7^2,\ Va + Ub = 25a + 22b$

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
-17	-403	-127	-359	-337	-1	-293	-271	-83	-227	-41	-61	-23	-139	-13	-19	-73		-29	-1	1	37
-16	-1		-167		-29		-41		-101		-79		-19		-1		-13		1		31
-15	-353	-331		-41			-221	-199			-19		-89	-67		-23	-1		43		
-14	-41		-71		-1				-19		-1		-1		-1		1		17		
-13	-101	-281	-37	-79	-43	-193	-19	-149	-127	-1	-83	-61		-17	1	1	1	71	31	23	137
-12	-139				-19		-73				-29		-1				37		59		
-11	-253	-11	-209	-187	-11	-143	-121	-11	-11	-11		-11	11	11	11	11	11	121	143	11	187
-10	-19		-23				-1		-13		-1		1				31		1		53
-9	-29	-181		-137	-23		-71	-1		-1	17		61	83		127	149		193	43	
-8	-89		-67		-1		-23		-1		1		43		13		29		109		131
-7	-17	-131	-109	-29	-13	-43		1	23	1	67	89	37		31	59	199	221	1	53	
-6	-1				-1		1				23		17				1		67		
-5	-103	-1	-59	-37		1	29	17	73		13	139	23	61		227	83	271	293		337
-4	-13		-17		1		1		1		71		31		23		137		53		181
-3	-53	-31		13	1		79	101		29	167		211	233		277	299		7	73	
-2	-1		1		1		13		37		1		59		1		1		23		103
-1	-1	19	41	1	17	107	43	151	173	13	31	239	29	283	61	109	349	53	131	83	437
0	11																				
1	47	23	13	113	1	157	179	67	223	1	89	289	311	37	71	377	19	421	443	31	487
2	1		29		1		17		31		73		1		19		53		13		1
3	97	17		163	37		229	251		59	317		361	383		61	449		493	103	
4	61		83		1		127		149		19		193		43		79		37		281
5	1	169	191	71		257	31	43	323		367	389	137	433		53	499	521	181		587
6	43				13		19				1		109				131		71		
7	197	73	241	263	19	307		13	373	79	139	439	461		101	527	61	571	593	41	
8	37		19		31		59		199		221		1		53		41		103		331
9	247	269		313	67		379	401		89	467		73	533		577	599		643	19	
10	17		79				101		1		41		67				13		167		89
11	11	319	341	121	11	407	143	451	473	11		11	187	583	121	209	649	671	11	143	737
12	23				41		227				271		293				337		359		
13	347	41	391	59	29	457	479	167	523	109	1	589		211	131	677	233	103	743	17	787
14	31		13		23				137		37		53		17		181		1		
15	397	419		463			529	551			617		661	683		727	107		793		
16	211		233		17		277		299		107		7		73		43		409		431
17	149	67	491	19	107	557	193	601	89	43	667	689	79	733	151	37		821	281	173	887

$q = 7^3$, $Va + Ub = 25a + 22b$

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
-17	-403	-127	-359	-337	-1	-293	-271	-83	-227	-41	-61	-23	-139	-13	-19	-73		-29	-1	1	37
-16	-1		-167		-29		-41		-101		-79		-19		-1		-13		1		31
-15	-353	-331		-41			-221	-199			-19		-89	-67		-23	-1		43		
-14	-41		-71		-1				-19		-1		-1		-1		1		17		
-13	-101	-281	-37	-79	-43	-193	-19	-149	-127	-1	-83	-61		-17	1	1	1	71	31	23	137
-12	-139				-19		-73				-29		-1				37		59		
-11	-253	-11	-209	-187	-11	-143	-121	-11	-11	-11		-11	11	11	11	11	11	121	143	11	187
-10	-19		-23				-1		-13		-1		1				31		1		53
-9	-29	-181		-137	-23		-71	-1		-1	17		61	83		127	149		193	43	
-8	-89		-67		-1		-23		-1		1		43		13		29		109		131
-7	-17	-131	-109	-29	-13	-43		1	23	1	67	89	37		31	59	199	221	1	53	
-6	-1				-1		1				23		17				1		67		
-5	-103	-1	-59	-37		1	29	17	73		13	139	23	61		227	83	271	293		337
-4	-13		-17		1		1		1		71		31		23		137		53		181
-3	-53	-31		13	1		79	101		29	167		211	233		277	299		7	73	
-2	-1		1		1		13		37		1		59		1		1		23		103
-1	-1	19	41	1	17	107	43	151	173	13	31	239	29	283	61	109	349	53	131	83	437
0	11																				
1	47	23	13	113	1	157	179	67	223	1	89	289	311	37	71	377	19	421	443	31	487
2	1		29		1		17		31		73		1		19		53		13		1
3	97	17		163	37		229	251		59	317		361	383		61	449		493	103	
4	61		83		1		127		149		19		193		43		79		37		281
5	1	169	191	71		257	31	43	323		367	389	137	433		53	499	521	181		587
6	43				13		19				1		109				131		71		
7	197	73	241	263	19	307		13	373	79	139	439	461		101	527	61	571	593	41	
8	37		19		31		59		199		221		1		53		41		103		331
9	247	269		313	67		379	401		89	467		73	533		577	599		643	19	
10	17		79				101		1		41		67				13		167		89
11	11	319	341	121	11	407	143	451	473	11		11	187	583	121	209	649	671	11	143	737
12	23				41		227				271		293				337		359		
13	347	41	391	59	29	457	479	167	523	109	1	589		211	131	677	233	103	743	17	787
14	31		13		23				137		37		53		17		181		1		
15	397	419		463			529	551			617		661	683		727	107		793		
16	211		233		17		277		299		107		7		73		43		409		431
17	149	67	491	19	107	557	193	601	89	43	667	689	79	733	151	37		821	281	173	887

$q = 7^3$, $Va + Ub = 25a + 22b$

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
-17	-403	-127	-359	-337	-1	-293	-271	-83	-227	-41	-61	-23	-139	-13	-19	-73		-29	-1	1	37
-16	-1		-167		-29		-41		-101		-79		-19		-1		-13		1		31
-15	-353	-331		-41			-221	-199			-19		-89	-67		-23	-1		43		
-14	-41		-71		-1				-19		-1		-1		-1		1		17		
-13	-101	-281	-37	-79	-43	-193	-19	-149	-127	-1	-83	-61		-17	1	1	1	71	31	23	137
-12	-139				-19		-73				-29		-1				37		59		
-11	-253	-11	-209	-187	-11	-143	-121	-11	-11	-11		-11	11	11	11	11	11	121	143	11	187
-10	-19		-23				-1		-13		-1		1				31		1		53
-9	-29	-181		-137	-23		-71	-1		-1	17		61	83		127	149		193	43	
-8	-89		-67		-1		-23		-1		1		43		13		29		109		131
-7	-17	-131	-109	-29	-13	-43		1	23	1	67	89	37		31	59	199	221	1	53	
-6	-1				-1		1				23		17				1		67		
-5	-103	-1	-59	-37		1	29	17	73		13	139	23	61		227	83	271	293		337
-4	-13		-17		1		1		1		71		31		23		137		53		181
-3	-53	-31		13	1		79	101		29	167		211	233		277	299		1	73	
-2	-1		1		1		13		37		1		59		1		1		23		103
-1	-1	19	41	1	17	107	43	151	173	13	31	239	29	283	61	109	349	53	131	83	437
0	11																				
1	47	23	13	113	1	157	179	67	223	1	89	289	311	37	71	377	19	421	443	31	487
2	1		29		1		17		31		73		1		19		53		13		1
3	97	17		163	37		229	251		59	317		361	383		61	449		493	103	
4	61		83		1		127		149		19		193		43		79		37		281
5	1	169	191	71		257	31	43	323		367	389	137	433		53	499	521	181		587
6	43				13		19				1		109				131		71		
7	197	73	241	263	19	307		13	373	79	139	439	461		101	527	61	571	593	41	
8	37		19		31		59		199		221		1		53		41		103		331
9	247	269		313	67		379	401		89	467		73	533		577	599		643	19	
10	17		79				101		1		41		67				13		167		89
11	11	319	341	121	11	407	143	451	473	11		11	187	583	121	209	649	671	11	143	737
12	23				41		227				271		293				337		359		
13	347	41	391	59	29	457	479	167	523	109	1	589		211	131	677	233	103	743	17	787
14	31		13		23				137		37		53		17		181		1		
15	397	419		463			529	551			617		661	683		727	107		793		
16	211		233		17		277		299		107		1		73		43		409		431
17	149	67	491	19	107	557	193	601	89	43	667	689	79	733	151	37		821	281	173	887

$q = 11$, $Va + Ub = 25a + 22b$

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
-17	-403	-127	-359	-337	-1	-293	-271	-83	-227	-41	-61	-23	-139	-13	-19	-73		-29	-1	1	37
-16	-1		-167		-29		-41		-101		-79		-19		-1		-13		1		31
-15	-353	-331		-41			-221	-199			-19		-89	-67		-23	-1		43		
-14	-41		-71		-1				-19		-1		-1		-1		1		17		
-13	-101	-281	-37	-79	-43	-193	-19	-149	-127	-1	-83	-61		-17	1	1	1	71	31	23	137
-12	-139				-19		-73				-29		-1				37		59		
-11	-253	-11	-209	-187	-11	-143	-121	-11	-11	-11		-11	11	11	11	11	11	121	143	11	187
-10	-19		-23				-1		-13		-1		1				31		1		53
-9	-29	-181		-137	-23		-71	-1		-1	17		61	83		127	149		193	43	
-8	-89		-67		-1		-23		-1		1		43		13		29		109		131
-7	-17	-131	-109	-29	-13	-43		1	23	1	67	89	37		31	59	199	221	1	53	
-6	-1				-1		1				23		17				1		67		
-5	-103	-1	-59	-37		1	29	17	73		13	139	23	61		227	83	271	293		337
-4	-13		-17		1		1		1		71		31		23		137		53		181
-3	-53	-31		13	1		79	101		29	167		211	233		277	299		1	73	
-2	-1		1		1		13		37		1		59		1		1		23		103
-1	-1	19	41	1	17	107	43	151	173	13	31	239	29	283	61	109	349	53	131	83	437
0	11																				
1	47	23	13	113	1	157	179	67	223	1	89	289	311	37	71	377	19	421	443	31	487
2	1		29		1		17		31		73		1		19		53		13		1
3	97	17		163	37		229	251		59	317		361	383		61	449		493	103	
4	61		83		1		127		149		19		193		43		79		37		281
5	1	169	191	71		257	31	43	323		367	389	137	433		53	499	521	181		587
6	43				13		19				1		109				131		71		
7	197	73	241	263	19	307		13	373	79	139	439	461		101	527	61	571	593	41	
8	37		19		31		59		199		221		1		53		41		103		331
9	247	269		313	67		379	401		89	467		73	533		577	599		643	19	
10	17		79				101		1		41		67				13		167		89
11	11	319	341	121	11	407	143	451	473	11		11	187	583	121	209	649	671	11	143	737
12	23				41		227				271		293				337		359		
13	347	41	391	59	29	457	479	167	523	109	1	589		211	131	677	233	103	743	17	787
14	31		13		23				137		37		53		17		181		1		
15	397	419		463			529	551			617		661	683		727	107		793		
16	211		233		17		277		299		107		1		73		43		409		431
17	149	67	491	19	107	557	193	601	89	43	667	689	79	733	151	37		821	281	173	887

$q = 11$, $Va + Ub = 25a + 22b$

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
-17	-403	-127	-359	-337	-1	-293	-271	-83	-227	-41	-61	-23	-139	-13	-19	-73		-29	-1	1	37
-16	-1		-167		-29		-41		-101		-79		-19		-1		-13		1		31
-15	-353	-331		-41			-221	-199			-19		-89	-67		-23	-1		43		
-14	-41		-71		-1				-19		-1		-1		-1		1		17		
-13	-101	-281	-37	-79	-43	-193	-19	-149	-127	-1	-83	-61		-17	1	1	1	71	31	23	137
-12	-139				-19		-73				-29		-1				37		59		
-11	-23	-1	-19	-17	-1	-13	-11	-1	-1	-1		-1	1	1	1	1	1	11	13	1	17
-10	-19		-23				-1		-13		-1		1				31		1		53
-9	-29	-181		-137	-23		-71	-1		-1	17		61	83		127	149		193	43	
-8	-89		-67		-1		-23		-1		1		43		13		29		109		131
-7	-17	-131	-109	-29	-13	-43		1	23	1	67	89	37		31	59	199	221	1	53	
-6	-1				-1		1				23		17				1		67		
-5	-103	-1	-59	-37		1	29	17	73		13	139	23	61		227	83	271	293		337
-4	-13		-17		1		1		1		71		31		23		137		53		181
-3	-53	-31		13	1		79	101		29	167		211	233		277	299		1	73	
-2	-1		1		1		13		37		1		59		1		1		23		103
-1	-1	19	41	1	17	107	43	151	173	13	31	239	29	283	61	109	349	53	131	83	437
0	1																				
1	47	23	13	113	1	157	179	67	223	1	89	289	311	37	71	377	19	421	443	31	487
2	1		29		1		17		31		73		1		19		53		13		1
3	97	17		163	37		229	251		59	317		361	383		61	449		493	103	
4	61		83		1		127		149		19		193		43		79		37		281
5	1	169	191	71		257	31	43	323		367	389	137	433		53	499	521	181		587
6	43				13		19				1		109				131		71		
7	197	73	241	263	19	307		13	373	79	139	439	461		101	527	61	571	593	41	
8	37		19		31		59		199		221		1		53		41		103		331
9	247	269		313	67		379	401		89	467		73	533		577	599		643	19	
10	17		79				101		1		41		67				13		167		89
11	1	29	31	11	1	37	13	41	43	1		1	17	53	11	19	59	61	1	13	67
12	23				41		227				271		293				337		359		
13	347	41	391	59	29	457	479	167	523	109	1	589		211	131	677	233	103	743	17	787
14	31		13		23				137		37		53		17		181		1		
15	397	419		463			529	551			617		661	683		727	107		793		
16	211		233		17		277		299		107		1		73		43		409		431
17	149	67	491	19	107	557	193	601	89	43	667	689	79	733	151	37		821	281	173	887

$q = 11^2,\ Va + Ub = 25a + 22b$

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
-17	-403	-127	-359	-337	-1	-293	-271	-83	-227	-41	-61	-23	-139	-13	-19	-73		-29	-1	1	37
-16	-1		-167		-29		-41		-101		-79		-19		-1		-13		1		31
-15	-353	-331		-41			-221	-199			-19		-89	-67		-23	-1		43		
-14	-41		-71		-1				-19		-1		-1		-1		1		17		
-13	-101	-281	-37	-79	-43	-193	-19	-149	-127	-1	-83	-61		-17	1	1	1	71	31	23	137
-12	-139				-19		-73				-29		-1				37		59		
-11	-23	-1	-19	-17	-1	-13	-11	-1	-1	-1		-1	1	1	1	1	1	11	13	1	17
-10	-19		-23				-1		-13		-1		1				31		1		53
-9	-29	-181		-137	-23		-71	-1		-1	17		61	83		127	149		193	43	
-8	-89		-67		-1		-23		-1		1		43		13		29		109		131
-7	-17	-131	-109	-29	-13	-43		1	23	1	67	89	37		31	59	199	221	1	53	
-6	-1				-1		1				23		17				1		67		
-5	-103	-1	-59	-37		1	29	17	73		13	139	23	61		227	83	271	293		337
-4	-13		-17		1		1		1		71		31		23		137		53		181
-3	-53	-31		13	1		79	101		29	167		211	233		277	299		1	73	
-2	-1		1		1		13		37		1		59		1		1		23		103
-1	-1	19	41	1	17	107	43	151	173	13	31	239	29	283	61	109	349	53	131	83	437
0	1																				
1	47	23	13	113	1	157	179	67	223	1	89	289	311	37	71	377	19	421	443	31	487
2	1		29		1		17		31		73		1		19		53		13		1
3	97	17		163	37		229	251		59	317		361	383		61	449		493	103	
4	61		83		1		127		149		19		193		43		79		37		281
5	1	169	191	71		257	31	43	323		367	389	137	433		53	499	521	181		587
6	43				13		19				1		109				131		71		
7	197	73	241	263	19	307		13	373	79	139	439	461		101	527	61	571	593	41	
8	37		19		31		59		199		221		1		53		41		103		331
9	247	269		313	67		379	401		89	467		73	533		577	599		643	19	
10	17		79				101		1		41		67				13		167		89
11	1	29	31	11	1	37	13	41	43	1		1	17	53	11	19	59	61	1	13	67
12	23				41		227				271		293				337		359		
13	347	41	391	59	29	457	479	167	523	109	1	589		211	131	677	233	103	743	17	787
14	31		13		23				137		37		53		17		181		1		
15	397	419		463			529	551			617		661	683		727	107		793		
16	211		233		17		277		299		107		1		73		43		409		431
17	149	67	491	19	107	557	193	601	89	43	667	689	79	733	151	37		821	281	173	887

$q = 11^2,\ Va + Ub = 25a + 22b$

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
-17	-403	-127	-359	-337	-1	-293	-271	-83	-227	-41	-61	-23	-139	-13	-19	-73		-29	-1	1	37
-16	-1		-167		-29		-41		-101		-79		-19		-1		-13		1		31
-15	-353	-331		-41			-221	-199			-19		-89	-67		-23	-1		43		
-14	-41		-71		-1				-19		-1		-1		-1		1		17		
-13	-101	-281	-37	-79	-43	-193	-19	-149	-127	-1	-83	-61		-17	1	1	1	71	31	23	137
-12	-139				-19		-73				-29		-1				37		59		
-11	-23	-1	-19	-17	-1	-13	-1	-1	-1	-1		-1	1	1	1	1	1	1	13	1	17
-10	-19		-23				-1		-13		-1		1				31		1		53
-9	-29	-181		-137	-23		-71	-1		-1	17		61	83		127	149		193	43	
-8	-89		-67		-1		-23		-1		1		43		13		29		109		131
-7	-17	-131	-109	-29	-13	-43		1	23	1	67	89	37		31	59	199	221	1	53	
-6	-1				-1		1				23		17				1		67		
-5	-103	-1	-59	-37		1	29	17	73		13	139	23	61		227	83	271	293		337
-4	-13		-17		1		1		1		71		31		23		137		53		181
-3	-53	-31		13	1		79	101		29	167		211	233		277	299		1	73	
-2	-1		1		1		13		37		1		59		1		1		23		103
-1	-1	19	41	1	17	107	43	151	173	13	31	239	29	283	61	109	349	53	131	83	437
0	1																				
1	47	23	13	113	1	157	179	67	223	1	89	289	311	37	71	377	19	421	443	31	487
2	1		29		1		17		31		73		1		19		53		13		1
3	97	17		163	37		229	251		59	317		361	383		61	449		493	103	
4	61		83		1		127		149		19		193		43		79		37		281
5	1	169	191	71		257	31	43	323		367	389	137	433		53	499	521	181		587
6	43				13		19				1		109				131		71		
7	197	73	241	263	19	307		13	373	79	139	439	461		101	527	61	571	593	41	
8	37		19		31		59		199		221		1		53		41		103		331
9	247	269		313	67		379	401		89	467		73	533		577	599		643	19	
10	17		79				101		1		41		67				13		167		89
11	1	29	31	1	1	37	13	41	43	1		1	17	53	1	19	59	61	1	13	67
12	23				41		227				271		293				337		359		
13	347	41	391	59	29	457	479	167	523	109	1	589		211	131	677	233	103	743	17	787
14	31		13		23				137		37		53		17		181		1		
15	397	419		463			529	551			617		661	683		727	107		793		
16	211		233		17		277		299		107		1		73		43		409		431
17	149	67	491	19	107	557	193	601	89	43	667	689	79	733	151	37		821	281	173	887

$q = 13$, $Va + Ub = 25a + 22b$

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
-17	-403	-127	-359	-337	-1	-293	-271	-83	-227	-41	-61	-23	-139	-13	-19	-73		-29	-1	1	37
-16	-1		-167		-29		-41		-101		-79		-19		-1		-13		1		31
-15	-353	-331		-41			-221	-199			-19		-89	-67		-23	-1		43		
-14	-41		-71		-1				-19		-1		-1		-1		1		17		
-13	-101	-281	-37	-79	-43	-193	-19	-149	-127	-1	-83	-61		-17	1	1	1	71	31	23	137
-12	-139				-19		-73				-29		-1				37		59		
-11	-23	-1	-19	-17	-1	-13	-1	-1	-1	-1		-1	1	1	1	1	1	1	13	1	17
-10	-19		-23				-1		-13		-1		1				31		1		53
-9	-29	-181		-137	-23		-71	-1		-1	17		61	83		127	149		193	43	
-8	-89		-67		-1		-23		-1		1		43		13		29		109		131
-7	-17	-131	-109	-29	-13	-43		1	23	1	67	89	37		31	59	199	221	1	53	
-6	-1				-1		1				23		17				1		67		
-5	-103	-1	-59	-37		1	29	17	73		13	139	23	61		227	83	271	293		337
-4	-13		-17		1		1		1		71		31		23		137		53		181
-3	-53	-31		13	1		79	101		29	167		211	233		277	299		1	73	
-2	-1		1		1		13		37		1		59		1		1		23		103
-1	-1	19	41	1	17	107	43	151	173	13	31	239	29	283	61	109	349	53	131	83	437
0	1																				
1	47	23	13	113	1	157	179	67	223	1	89	289	311	37	71	377	19	421	443	31	487
2	1		29		1		17		31		73		1		19		53		13		1
3	97	17		163	37		229	251		59	317		361	383		61	449		493	103	
4	61		83		1		127		149		19		193		43		79		37		281
5	1	169	191	71		257	31	43	323		367	389	137	433		53	499	521	181		587
6	43				13		19				1		109				131		71		
7	197	73	241	263	19	307		13	373	79	139	439	461		101	527	61	571	593	41	
8	37		19		31		59		199		221		1		53		41		103		331
9	247	269		313	67		379	401		89	467		73	533		577	599		643	19	
10	17		79				101		1		41		67				13		167		89
11	1	29	31	1	1	37	13	41	43	1		1	17	53	1	19	59	61	1	13	67
12	23				41		227				271		293				337		359		
13	347	41	391	59	29	457	479	167	523	109	1	589		211	131	677	233	103	743	17	787
14	31		13		23				137		37		53		17		181		1		
15	397	419		463			529	551			617		661	683		727	107		793		
16	211		233		17		277		299		107		1		73		43		409		431
17	149	67	491	19	107	557	193	601	89	43	667	689	79	733	151	37		821	281	173	887

$q = 13$, $Va + Ub = 25a + 22b$

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
-17	-31	-127	-359	-337	-1	-293	-271	-83	-227	-41	-61	-23	-139	-1	-19	-73		-29	-1	1	37
-16	-1		-167		-29		-41		-101		-79		-19		-1		-1		1		31
-15	-353	-331		-41			-17	-199			-19		-89	-67		-23	-1		43		
-14	-41		-71		-1				-19		-1		-1		-1		1		17		
-13	-101	-281	-37	-79	-43	-193	-19	-149	-127	-1	-83	-61		-17	1	1	1	71	31	23	137
-12	-139				-19		-73				-29		-1				37		59		
-11	-23	-1	-19	-17	-1	-1	-1	-1	-1	-1		-1	1	1	1	1	1	1	1	1	17
-10	-19		-23				-1		-1		-1		1				31		1		53
-9	-29	-181		-137	-23		-71	-1		-1	17		61	83		127	149		193	43	
-8	-89		-67		-1		-23		-1		1		43		1		29		109		131
-7	-17	-131	-109	-29	-1	-43		1	23	1	67	89	37		31	59	199	17	1	53	
-6	-1				-1		1				23		17				1		67		
-5	-103	-1	-59	-37		1	29	17	73		1	139	23	61		227	83	271	293		337
-4	-1		-17		1		1		1		71		31		23		137		53		181
-3	-53	-31		1	1		79	101		29	167		211	233		277	23		1	73	
-2	-1		1		1		1		37		1		59		1		1		23		103
-1	-1	19	41	1	17	107	43	151	173	1	31	239	29	283	61	109	349	53	131	83	437
0	1																				
1	47	23	1	113	1	157	179	67	223	1	89	289	311	37	71	29	19	421	443	31	487
2	1		29		1		17		31		73		1		19		53		1		1
3	97	17		163	37		229	251		59	317		361	383		61	449		493	103	
4	61		83		1		127		149		19		193		43		79		37		281
5	1	13	191	71		257	31	43	323		367	389	137	433		53	499	521	181		587
6	43				1		19				1		109				131		71		
7	197	73	241	263	19	307		1	373	79	139	439	461		101	527	61	571	593	41	
8	37		19		31		59		199		17		1		53		41		103		331
9	19	269		313	67		379	401		89	467		73	41		577	599		643	19	
10	17		79				101		1		41		67				1		167		89
11	1	29	31	1	1	37	1	41	43	1		1	17	53	1	19	59	61	1	1	67
12	23				41		227				271		293				337		359		
13	347	41	391	59	29	457	479	167	523	109	1	589		211	131	677	233	103	743	17	787
14	31		1		23				137		37		53		17		181		1		
15	397	419		463			529	551			617		661	683		727	107		61		
16	211		233		17		277		23		107		1		73		43		409		431
17	149	67	491	19	107	557	193	601	89	43	667	53	79	733	151	37		821	281	173	887

$q = 13^2,\ Va + Ub = 25a + 22b$

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
-17	-31	-127	-359	-337	-1	-293	-271	-83	-227	-41	-61	-23	-139	-1	-19	-73		-29	-1	1	37
-16	-1		-167		-29		-41		-101		-79		-19		-1		-1		1		31
-15	-353	-331		-41			-17	-199			-19		-89	-67		-23	-1		43		
-14	-41		-71		-1				-19		-1		-1		-1		1		17		
-13	-101	-281	-37	-79	-43	-193	-19	-149	-127	-1	-83	-61		-17	1	1	1	71	31	23	137
-12	-139				-19		-73				-29		-1				37		59		
-11	-23	-1	-19	-17	-1	-1	-1	-1	-1	-1		-1	1	1	1	1	1	1	1	1	17
-10	-19		-23				-1		-1		-1		1				31		1		53
-9	-29	-181		-137	-23		-71	-1		-1	17		61	83		127	149		193	43	
-8	-89		-67		-1		-23		-1		1		43		1		29		109		131
-7	-17	-131	-109	-29	-1	-43		1	23	1	67	89	37		31	59	199	17	1	53	
-6	-1				-1		1				23		17				1		67		
-5	-103	-1	-59	-37		1	29	17	73		1	139	23	61		227	83	271	293		337
-4	-1		-17		1		1		1		71		31		23		137		53		181
-3	-53	-31		1	1		79	101		29	167		211	233		277	23		1	73	
-2	-1		1		1		1		37		1		59		1		1		23		103
-1	-1	19	41	1	17	107	43	151	173	1	31	239	29	283	61	109	349	53	131	83	437
0	1																				
1	47	23	1	113	1	157	179	67	223	1	89	289	311	37	71	29	19	421	443	31	487
2	1		29		1		17		31		73		1		19		53		1		1
3	97	17		163	37		229	251		59	317		361	383		61	449		493	103	
4	61		83		1		127		149		19		193		43		79		37		281
5	1	13	191	71		257	31	43	323		367	389	137	433		53	499	521	181		587
6	43				1		19				1		109				131		71		
7	197	73	241	263	19	307		1	373	79	139	439	461		101	527	61	571	593	41	
8	37		19		31		59		199		17		1		53		41		103		331
9	19	269		313	67		379	401		89	467		73	41		577	599		643	19	
10	17		79				101		1		41		67				1		167		89
11	1	29	31	1	1	37	1	41	43	1		1	17	53	1	19	59	61	1	1	67
12	23				41		227				271		293				337		359		
13	347	41	391	59	29	457	479	167	523	109	1	589		211	131	677	233	103	743	17	787
14	31		1		23				137		37		53		17		181		1		
15	397	419		463			529	551			617		661	683		727	107		61		
16	211		233		17		277		23		107		1		73		43		409		431
17	149	67	491	19	107	557	193	601	89	43	667	53	79	733	151	37		821	281	173	887

$q = 13^2,\ Va + Ub = 25a + 22b$

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
-17	-31	-127	-359	-337	-1	-293	-271	-83	-227	-41	-61	-23	-139	-1	-19	-73		-29	-1	1	37
-16	-1		-167		-29		-41		-101		-79		-19		-1		-1		1		31
-15	-353	-331		-41			-17	-199			-19		-89	-67		-23	-1		43		
-14	-41		-71		-1				-19		-1		-1		-1		1		17		
-13	-101	-281	-37	-79	-43	-193	-19	-149	-127	-1	-83	-61		-17	1	1	1	71	31	23	137
-12	-139				-19		-73				-29		-1				37		59		
-11	-23	-1	-19	-17	-1	-1	-1	-1	-1	-1		-1	1	1	1	1	1	1	1	1	17
-10	-19		-23				-1		-1		-1		1				31		1		53
-9	-29	-181		-137	-23		-71	-1		-1	17		61	83		127	149		193	43	
-8	-89		-67		-1		-23		-1		1		43		1		29		109		131
-7	-17	-131	-109	-29	-1	-43		1	23	1	67	89	37		31	59	199	17	1	53	
-6	-1				-1		1				23		17				1		67		
-5	-103	-1	-59	-37		1	29	17	73		1	139	23	61		227	83	271	293		337
-4	-1		-17		1		1		1		71		31		23		137		53		181
-3	-53	-31		1	1		79	101		29	167		211	233		277	23		1	73	
-2	-1		1		1		1		37		1		59		1		1		23		103
-1	-1	19	41	1	17	107	43	151	173	1	31	239	29	283	61	109	349	53	131	83	437
0	1																				
1	47	23	1	113	1	157	179	67	223	1	89	289	311	37	71	29	19	421	443	31	487
2	1		29		1		17		31		73		1		19		53		1		1
3	97	17		163	37		229	251		59	317		361	383		61	449		493	103	
4	61		83		1		127		149		19		193		43		79		37		281
5	1	1	191	71		257	31	43	323		367	389	137	433		53	499	521	181		587
6	43				1		19				1		109				131		71		
7	197	73	241	263	19	307		1	373	79	139	439	461		101	527	61	571	593	41	
8	37		19		31		59		199		17		1		53		41		103		331
9	19	269		313	67		379	401		89	467		73	41		577	599		643	19	
10	17		79				101		1		41		67				1		167		89
11	1	29	31	1	1	37	1	41	43	1		1	17	53	1	19	59	61	1	1	67
12	23				41		227				271		293				337		359		
13	347	41	391	59	29	457	479	167	523	109	1	589		211	131	677	233	103	743	17	787
14	31		1		23				137		37		53		17		181		1		
15	397	419		463			529	551			617		661	683		727	107		61		
16	211		233		17		277		23		107		1		73		43		409		431
17	149	67	491	19	107	557	193	601	89	43	667	53	79	733	151	37		821	281	173	887

Survivors: (a, b) s.t. $T[a+A][b-1] = \pm 1$

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
-17	-31	-127	-359	-337	-1	-293	-271	-83	-227	-41	-61	-23	-139	-1	-19	-73		-29	-1	1	37
-16	-1		-167		-29		-41		-101		-79		-19		-1		-1		1		31
-15	-353	-331		-41			-17	-199			-19		-89	-67		-23	-1		43		
-14	-41		-71		-1				-19		-1		-1		-1		1		17		
-13	-101	-281	-37	-79	-43	-193	-19	-149	-127	-1	-83	-61		-17	1	1	1	71	31	23	137
-12	-139				-19		-73				-29		-1				37		59		
-11	-23	-1	-19	-17	-1	-1	-1	-1	-1	-1		-1	1	1	1	1	1	1	1	1	17
-10	-19		-23				-1		-1		-1		1				31		1		53
-9	-29	-181		-137	-23		-71	-1		-1	17		61	83		127	149		193	43	
-8	-89		-67		-1		-23		-1		1		43		1		29		109		131
-7	-17	-131	-109	-29	-1	-43		1	23	1	67	89	37		31	59	199	17	1	53	
-6	-1				-1		1				23		17				1		67		
-5	-103	-1	-59	-37		1	29	17	73		1	139	23	61		227	83	271	293		337
-4	-1		-17		1		1		1		71		31		23		137		53		181
-3	-53	-31		1	1		79	101		29	167		211	233		277	23		1	73	
-2	-1		1		1		1		37		1		59		1		1		23		103
-1	-1	19	41	1	17	107	43	151	173	1	31	239	29	283	61	109	349	53	131	83	437
0	1																				
1	47	23	1	113	1	157	179	67	223	1	89	289	311	37	71	29	19	421	443	31	487
2	1		29		1		17		31		73		1		19		53		1		1
3	97	17		163	37		229	251		59	317		361	383		61	449		493	103	
4	61		83		1		127		149		19		193		43		79		37		281
5	1	1	191	71		257	31	43	323		367	389	137	433		53	499	521	181		587
6	43				1		19				1		109				131		71		
7	197	73	241	263	19	307		1	373	79	139	439	461		101	527	61	571	593	41	
8	37		19		31		59		199		17		1		53		41		103		331
9	19	269		313	67		379	401		89	467		73	41		577	599		643	19	
10	17		79				101		1		41		67				1		167		89
11	1	29	31	1	1	37	1	41	43	1		1	17	53	1	19	59	61	1	1	67
12	23				41		227				271		293				337		359		
13	347	41	391	59	29	457	479	167	523	109	1	589		211	131	677	233	103	743	17	787
14	31		1		23				137		37		53		17		181		1		
15	397	419		463			529	551			617		661	683		727	107		61		
16	211		233		17		277		23		107		1		73		43		409		431
17	149	67	491	19	107	557	193	601	89	43	667	53	79	733	151	37		821	281	173	887

Sieve: Coppersmith–Odlyzko–Schroeppel 1986

114 (a, b) pairs "survivors" after sieving

In practice:

- store log of norms (much smaller, `float` vs `mpz_t`)
- sieve for $q \leq$ sieving bound
- substract $\log q$ for each hit
- recompute and factor $aU + bV$ (ECM) for each $T[a + A][b + 1] \leq$ given cofactor bound
- if smooth $aU + bV$, compute and factor $a^2 + b^2$

SageMath experimentation

```
example-1109-COS.sage
example-1109-quadratic.sage
```

$\mathbb{Z}[i]$ is the ring of integers of $\mathbb{Q}(i) = \mathbb{Q}[x]/(x^2 + 1)$
NFS setting:
$f = x^2 + 1$, $g = vx - u$ where $f(u/v) = 0 \bmod p$

We can do everything with $\mathbb{Z}[\sqrt{-5}]$, norm $a^2 + 5b^2$,
$f = x^2 + 5$, $g = tx - s$ where $f(s/t) = 0 \bmod p$
Homework:
run the Sage code with $p = 1109$ and $f = x^2 + 5$.
What is the second polynomial, $g(x)$?

SageMath experimentation

example-1109-COS.sage
example-1109-quadratic.sage

$\mathbb{Z}[i]$ is the ring of integers of $\mathbb{Q}(i) = \mathbb{Q}[x]/(x^2+1)$
NFS setting:
$f = x^2 + 1$, $g = vx - u$ where $f(u/v) = 0 \bmod p$

We can do everything with $\mathbb{Z}[\sqrt{-5}]$, norm $a^2 + 5b^2$,
$f = x^2 + 5$, $g = tx - s$ where $f(s/t) = 0 \bmod p$
Homework:
run the Sage code with $p = 1109$ and $f = x^2 + 5$.
What is the second polynomial, $g(x)$?
$p = 33^2 + 5 \cdot 2^2$, $\sqrt{-5} = 33/2 \bmod p$
$f(33/2) = 0 \bmod p$, $g = 2(x - 33/2) = 2x - 33$

SageMath experimentation

`example-1109-COS.sage`
`example-1109-quadratic.sage`

$\mathbb{Z}[i]$ is the ring of integers of $\mathbb{Q}(i) = \mathbb{Q}[x]/(x^2+1)$
NFS setting:
$f = x^2 + 1$, $g = vx - u$ where $f(u/v) = 0 \bmod p$

We can do everything with $\mathbb{Z}[\sqrt{-5}]$, norm $a^2 + 5b^2$,
$f = x^2 + 5$, $g = tx - s$ where $f(s/t) = 0 \bmod p$
Homework:
run the Sage code with $p = 1109$ and $f = x^2 + 5$.
What is the second polynomial, $g(x)$?
$p = 33^2 + 5 \cdot 2^2$, $\sqrt{-5} = 33/2 \bmod p$
$f(33/2) = 0 \bmod p$, $g = 2(x - 33/2) = 2x - 33$

What is the factor basis on the algebraic side?
What are the "primes"?

Example in $\mathbb{Z}[i]$: individual log

We managed to factor numbers of size bounded by $A\sqrt{p}$
We obtained the logarithms of $\{2, 3, 5, 7, 11, 13\}$ in basis $g = 2$, mod $p - 1$
$\boldsymbol{v} = [1, 219, 594, 311, 910, 1100] \bmod p - 1$

Target 314, generator $g = 2$
Search for smooth $g^s h \mod p$
But has size p

Example in $\mathbb{Z}[i]$: individual log

We managed to factor numbers of size bounded by $A\sqrt{p}$
We obtained the logarithms of $\{2, 3, 5, 7, 11, 13\}$ in basis $g = 2$, mod $p - 1$
$\boldsymbol{v} = [1, 219, 594, 311, 910, 1100] \bmod p - 1$

Target 314, generator $g = 2$
Search for smooth $g^s h \mod p$
But has size p
Rational Reconstruction
write $g^s h \mod p = u/v \bmod p$
where $u, v \approx \sqrt{p}$
(Troncated Xgcd)
Seach for smooth u, v at the same time

Example in $\mathbb{Z}[i]$: individual log

We managed to factor numbers of size bounded by $A\sqrt{p}$
We obtained the logarithms of $\{2, 3, 5, 7, 11, 13\}$ in basis $g = 2$, mod $p - 1$
$\boldsymbol{v} = [1, 219, 594, 311, 910, 1100]$ mod $p - 1$

Target 314, generator $g = 2$
Search for smooth $g^s h \mod p$
But has size p
Rational Reconstruction
write $g^s h \mod p = u/v \bmod p$
where $u, v \approx \sqrt{p}$
(Troncated Xgcd)
Seach for smooth u, v at the same time
$314 = -20/7 \bmod p = -2^2 \cdot 5/7$

$$\begin{aligned} \log_g 314 &= \log_g -1 + 2\log_g 2 + \log_g 5 - \log_g 7 \\ &= (p-1)/2 + 2 + 594 - 311 \bmod p - 1 \\ &= 839 \end{aligned}$$

$2^{839} = 314 \bmod p$

COS with $\mathbb{Z}[i]$: running-time

Input: p prime, generator g, target h
Output: database of $\log p_i$ for $p_i \leq B$ small primes, $\log_g h$

- select polynomials: easy
  $f = x^2 + d$, $g = Vx - U$, $U/V = m$, $f(m) = g(m) = 0 \bmod p$
- enumerate pairs (a, b): $A(2A+1) \approx A^2$ pairs
  - factor $N_a = a^2 + db^2$, $N_r = Va + Ub$
  - sieve up to a bound $B' < B$
  - factor with Elliptic Curve Method (ECM)
    $e^{\sqrt{(2+o(1)) \log B \log\log B}} (\log N)^2 = L_B(\sqrt{2})(\log N)^2$
- compute right kernel of sparse matrix $2B$ rows, $2B$ columns ($4B^2$ cells) Lanczos, block-Wiedemann $O(B^2)$
  $\rightarrow$ obtain database of $\log p_i$ for prime $p_i \leq B$
- individual discrete log
  - find s s.t. $g^s \cdot h = u/v \bmod p$ and u, v are B-smooth
  - compute $\log_g h$ from above: now easy

From COS Sieve to General-NFS

https://gitlab.inria.fr/dldb/discretelogdb

Date	authors	size	algo	polynomials
02.10.1995	Weber et al.	65dd, 215b	NFS	base-m
25.03.1996	Weber et al.	75dd, 248b	NFS	base-m
25.11.1996	Weber et al.	85dd, 281b	COS	x^2+2
25.01.1998	Weber Denny	129dd, 427b	SNFS	$739x^5-5152, x-7^{30}$
26.08.1998	Joux Lercier	90dd, 298b	COS	x^2+2
01.11.1999	Joux Lercier	100dd, 331b	NFS	x^3+2
19.01.2001	Joux Lercier	110dd, 364b	NFS	$x^3-12x^2-9x+12$
17.04.2001	Joux Lercier	120dd, 397b	NFS	x^3-9x^2-9x+9
18.06.2005	Joux Lercier	130dd, 431b	NFS	$x^3+12x^2-13x+3$
23.08.2006	JL+Smart Vercauteren	119dd, 394b	NFS	$f=x^3+x^2-2x-1$ $g=f+p$, $\mathbb{F}_{p^3}$
22.12.2006	Matyukhin et al.	135dd, 448b	NFS	x^3+9x^2-x+3
05.02.2007	Kleinjung	160dd, 530b	NFS	skewed base-m
16.01.2016	Kleinjung et al.	232dd, 768b	NFS	$140x^4+34x^3+86x^2+5x-55$

Weber Denny Zayer record computations in $\mathbb{F}_p$

`https://listserv.nodak.edu/cgi-bin/wa.exe?A2=NMBRTHRY;30bf3766.9611`

Date: Mon, 25 Nov 1996 09:05:26 -0500

$p = 31081938080419611412191112051968261019660101 19\backslash$
$\quad 64030919711805194127121970060719120 7059$
$\quad$ 85 dd, 281 bits, $(p-1)/2$ is prime

$f = x^2 + 2$

$g = 1323274340819980392303558671985532821598359x$
$\quad +8237532479357539733978757237386763941 83967$

Target:

$h = 3141592653589793238462643383279502884197169399\backslash$
$\quad 37510582097494459230781640628620899862$

Weber Denny Zayer record computations in $\mathbb{F}_p$

`https://listserv.nodak.edu/cgi-bin/wa.exe?A2=`
`NMBRTHRY;30bf3766.9611`

Date: Mon, 25 Nov 1996 09:05:26 -0500

Smoothing:

$$h = \frac{-11079110202452842718953369487679257497634 03}{12383853456341283587269734548824840418 3959}$$

$$= \frac{-7 \cdot 61 \cdot 259463939167513881005933711655251932 0289}{13 \cdot 2207 \cdot 3779 \cdot 5053313 \cdot 38665007 \cdot 78959357 \cdot 74034701813} \bmod p$$

$$2594639391675138810059337116552519320289 =$$

$$\frac{33613 \cdot 40829 \cdot 83617 \cdot 851761 \cdot 2115961 \cdot 2443219 \cdot 4287211 \cdot 4976687}{4 \cdot 19 \cdot 6803 \cdot 8387 \cdot 59387 \cdot 152239 \cdot 586501 \cdot 628997 \cdot 18636193 \cdot 210112139} \bmod p$$

$$74034701813 =$$

$$\frac{-3 \cdot 17 \cdot 37 \cdot 1109 \cdot 6199 \cdot 24989 \cdot 46957 \cdot 120661 \cdot 936667 \cdot 4133219 \cdot 515357041}{2^{30} \cdot 5^{29} \cdot 13 \cdot 727 \cdot 1303 \cdot 2399 \cdot 9157 \cdot 32251 \cdot 630299 \cdot 3862493 \cdot 5308663 \cdot 422591069} \bmod p$$

Plan

Introduction

Index calculus algorithm

Coppersmith–Odlyzko–Schroeppel 1986

Factorization into prime ideals in quadratic number fields

Number Field Sieve with base-m

Number Field Sieve today: Joux–Lercier

Reference for this section

I. N. Stewart and D. O. Tall.
Algebraic Number Theory and Fermat's Last Theorem.
Chapman and Hall/CRC, 4th edition, October 2015.
Textbook - 322 Pages - 21 B/W Illustrations.

Chapter 4: Factorization into irreducibles

Quadratic number field

For $d \neq 0$ square-free,
$d \geq 1$, $K = \mathbb{Q}(\sqrt{-d})$ is a imaginary quadratic number field.
$d > 1$, $K = \mathbb{Q}(\sqrt{d})$ is a real quadratic number field.

Quadratic number field

For $d \neq 0$ square-free,
$d \geq 1$, $K = \mathbb{Q}(\sqrt{-d})$ is a imaginary quadratic number field.
$d > 1$, $K = \mathbb{Q}(\sqrt{d})$ is a real quadratic number field.

Definition (Algebraic integer)

$a \in K$ is such that there exists a **monic** polynomial P_a of integer coefficients s.t. $P_a(a) = 0$ in K.

Quadratic number field

For $d \neq 0$ square-free,
$d \geq 1$, $K = \mathbb{Q}(\sqrt{-d})$ is a imaginary quadratic number field.
$d > 1$, $K = \mathbb{Q}(\sqrt{d})$ is a real quadratic number field.

Definition (Algebraic integer)

$a \in K$ is such that there exists a **monic** polynomial P_a of integer coefficients s.t. $P_a(a) = 0$ in K.

Definition (Norm in $K = \mathbb{Q}(\sqrt{-d})$, $d > 0$ square-free)

$\mathrm{Norm}(a + b\sqrt{-d}) = (a + b\sqrt{-d})(a - b\sqrt{-d}) = a^2 + db^2$

Quadratic number field

For $d \neq 0$ square-free,
$d \geq 1$, $K = \mathbb{Q}(\sqrt{-d})$ is a imaginary quadratic number field.
$d > 1$, $K = \mathbb{Q}(\sqrt{d})$ is a real quadratic number field.

Definition (Algebraic integer)

$a \in K$ is such that there exists a **monic** polynomial P_a of integer coefficients s.t. $P_a(a) = 0$ in K.

Definition (Norm in $K = \mathbb{Q}(\sqrt{-d})$, $d > 0$ square-free)

$\text{Norm}(a + b\sqrt{-d}) = (a + b\sqrt{-d})(a - b\sqrt{-d}) = a^2 + db^2$

Definition (Ring of algebraic integers of $K = \mathbb{Q}(\sqrt{-d})$)

- $\mathbb{Z}[\sqrt{-d}] = \{a + b\sqrt{-d},\ a, b \in \mathbb{Z}\}$ if $-d \equiv 3 \bmod 4$
- $\mathbb{Z}[(1 + \sqrt{-d})/2] = \{a/2 + b/2\sqrt{-d},\ a, b \in \mathbb{Z}\}$ if $-d \equiv 1 \bmod 4$

Quadratic number field

For $d \neq 0$ square-free,
$d \geq 1$, $K = \mathbb{Q}(\sqrt{-d})$ is a imaginary quadratic number field.
$d > 1$, $K = \mathbb{Q}(\sqrt{d})$ is a real quadratic number field.

Definition (Algebraic integer)

$a \in K$ is such that there exists a **monic** polynomial P_a of integer coefficients s.t. $P_a(a) = 0$ in K.

Definition (Norm in $K = \mathbb{Q}(\sqrt{-d})$, $d > 0$ square-free)

$\text{Norm}(a + b\sqrt{-d}) = (a + b\sqrt{-d})(a - b\sqrt{-d}) = a^2 + db^2$

Definition (Ring of algebraic integers of $K = \mathbb{Q}(\sqrt{-d})$)

- $\mathbb{Z}[\sqrt{-d}] = \{a + b\sqrt{-d},\ a, b \in \mathbb{Z}\}$ if $-d \equiv 3 \bmod 4$
- $\mathbb{Z}[(1 + \sqrt{-d})/2] = \{a/2 + b/2\sqrt{-d},\ a, b \in \mathbb{Z}\}$ if $-d \equiv 1 \bmod 4$

Definition (Unit)

u is a unit $\iff$ u is an algebraic integer and $\text{Norm}(u) = \pm 1$

The problem of non-unique factorization in $\mathbb{Z}[\sqrt{-5}]$

We have $6 = (1+\sqrt{-5})(1-\sqrt{-5}) = 2 \cdot 3$
There is no algebraic integer of norm 2 nor 3
(solve $a^2 + 5b^2 = 2$, $a'^2 + 5b'^2 = 3$: no solution)
We need a **unique factorization** in $\mathbb{Z}[\sqrt{-5}]$

Let $x \in \mathbb{Z}[\sqrt{-5}]$ not 0, not a unit.

- x is irreducible $\iff (x = st \implies s = u \text{ or } t = u)$, u unit
- x is prime $\iff (x \mid st \implies x \mid s \text{ or } x \mid t)$

irreducible $\neq$ prime

- do not consider algebraic integers but **ideals**
- compute a set of **two generators**

Computing two-element representation of an ideal

Input: prime ℓ, $K = \mathbb{Q}(\theta)$ number field
Wanted: $a - b\theta \in \mathbb{Z}[\theta]$ s.t. $\ell \mid \mathrm{Norm}(a - b\theta)$

Computing two-element representation of an ideal

Input: prime ℓ, $K = \mathbb{Q}(\theta)$ number field
Wanted: $a - b\theta \in \mathbb{Z}[\theta]$ s.t. $\ell \mid \mathrm{Norm}(a - b\theta)$

K defined by an irreducible monic polynomial $f(x)$
Wanted: $\iff \ell \mid \mathrm{Res}(a - bx, f(x))$

Computing two-element representation of an ideal

Input: prime ℓ, $K = \mathbb{Q}(\theta)$ number field
Wanted: $a - b\theta \in \mathbb{Z}[\theta]$ s.t. $\ell \mid \mathrm{Norm}(a - b\theta)$

K defined by an irreducible monic polynomial $f(x)$
Wanted: $\iff \ell \mid \mathrm{Res}(a - bx, f(x))$

$\iff \mathrm{Res}(a - bx, f(x)) = 0 \bmod \ell$
if $\ell \nmid b$, set $r = -a/b$
$\mathrm{Res}(r + x \bmod \ell, f(x) \bmod \ell) = 0$

Computing two-element representation of an ideal

Input: prime ℓ, $K = \mathbb{Q}(\theta)$ number field
Wanted: $a - b\theta \in \mathbb{Z}[\theta]$ s.t. $\ell \mid \mathrm{Norm}(a - b\theta)$

K defined by an irreducible monic polynomial $f(x)$
Wanted: $\iff \ell \mid \mathrm{Res}(a - bx, f(x))$

$\iff \mathrm{Res}(a - bx, f(x)) = 0 \bmod \ell$
if $\ell \nmid b$, set $r = -a/b$
$\mathrm{Res}(r + x \bmod \ell, f(x) \bmod \ell) = 0$

$\implies r + x$ is a factor of $f(x) \bmod \ell$
Let's factor $f(x)$ modulo ℓ

Computing two-element representation of an ideal

Input: prime ℓ, $K = \mathbb{Q}(\theta)$ number field
Wanted: $a - b\theta \in \mathbb{Z}[\theta]$ s.t. $\ell \mid \mathrm{Norm}(a - b\theta)$

K defined by an irreducible monic polynomial $f(x)$
Wanted: $\iff \ell \mid \mathrm{Res}(a - bx, f(x))$

$\iff \mathrm{Res}(a - bx, f(x)) = 0 \bmod \ell$
if $\ell \nmid b$, set $r = -a/b$
$\mathrm{Res}(r + x \bmod \ell, f(x) \bmod \ell) = 0$

$\implies r + x$ is a factor of $f(x)$ mod ℓ
Let's factor $f(x)$ modulo ℓ

For each degree one factor $r_i + x$ of $f(x)$ mod ℓ,
we have $\ell \mid \mathrm{Norm}(r_i + \theta)$.

Factorization into prime ideals

K number field defined by $f(x)$ over $\mathbb{Q}$

For ℓ prime integer $\in \mathbb{N}$,

Factor $f(x) \mod \ell$

Each distinct degree 1 factor $\longleftrightarrow$ one prime ideal of degree 1

$f = x^2 + 5$

ℓ	$f(x)$ mod ℓ	prime ideals of degree 1
2	$(x+1)^2$	$(2, x+1)$
3	$(x+1)(x-1)$	$(3, x+1), (3, x-1)$
5	x^2	$(5, x)$
7	$(x+3)(x-3)$	$(7, x+3), (7, x-3)$
11	x^2+5	(11)
13	x^2+5	(13)

Factorization into prime ideals

K number field defined by $f(x)$ over $\mathbb{Q}$
For ℓ prime integer $\in \mathbb{N}$,
Factor $f(x) \mod \ell$
Each distinct degree 1 factor $\longleftrightarrow$ one prime ideal of degree 1

$f = x^2 + 5$

ℓ	$f(x)$ mod ℓ	prime ideals of degree 1
2	$(x+1)^2$	$(2, x+1)$
3	$(x+1)(x-1)$	$(3, x+1), (3, x-1)$
5	x^2	$(5, x)$
7	$(x+3)(x-3)$	$(7, x+3), (7, x-3)$
11	x^2+5	(11)
13	x^2+5	(13)

inert

(11)
|
11

Factorization into prime ideals

K number field defined by $f(x)$ over $\mathbb{Q}$
For ℓ prime integer $\in \mathbb{N}$,
Factor $f(x) \mod \ell$
Each distinct degree 1 factor $\longleftrightarrow$ one prime ideal of degree 1

$f = x^2 + 5$

ℓ	$f(x) \bmod \ell$	prime ideals of degree 1
2	$(x+1)^2$	$(2, x+1)$
3	$(x+1)(x-1)$	$(3, x+1), (3, x-1)$
5	x^2	$(5, x)$
7	$(x+3)(x-3)$	$(7, x+3), (7, x-3)$
11	x^2+5	(11)
13	x^2+5	(13)

inert	**ramified**
(11)	$(2, x+1)$
|	|
11	2

Factorization into prime ideals

K number field defined by $f(x)$ over $\mathbb{Q}$
For ℓ prime integer $\in \mathbb{N}$,
Factor $f(x) \mod \ell$
Each distinct degree 1 factor $\longleftrightarrow$ one prime ideal of degree 1

$f = x^2 + 5$

ℓ	$f(x)$ mod ℓ	prime ideals of degree 1
2	$(x+1)^2$	$(2, x+1)$
3	$(x+1)(x-1)$	$(3, x+1), (3, x-1)$
5	x^2	$(5, x)$
7	$(x+3)(x-3)$	$(7, x+3), (7, x-3)$
11	x^2+5	(11)
13	x^2+5	(13)

inert	**ramified**	**split**
(11)	$(2, x+1)$	$(3, x+1)$, $(3, x-1)$
|	|	\\ /
11	2	3

Factorization into prime ideals

For $a - b\theta$ in $\mathbb{Z}[\theta]$,

1. compute $n = \text{Norm}(a - b\theta)$
2. factor n in $\mathbb{Z}$
3. match each prime factor ℓ of n with a prime ideal:
   compute $\gcd(\underbrace{f(x) \bmod \ell}_{=(x+s)(x+t)}, a - bx \bmod \ell)$

Factorization into prime ideals

For $a - b\theta$ in $\mathbb{Z}[\theta]$,

1. compute $n = \text{Norm}(a - b\theta)$
2. factor n in $\mathbb{Z}$
3. match each prime factor ℓ of n with a prime ideal:
   compute $\gcd(\underbrace{f(x) \bmod \ell}_{=(x+s)(x+t)}, a - bx \bmod \ell)$

$\theta = \sqrt{-5}$, $(a, b) = (1, 2)$, $a - b\theta = 1 - 2\sqrt{-5}$

$\text{Norm}(1 - 2\theta) = 1^2 + 5 \cdot 2^2 = 21 = 3 \cdot 7$
$\gcd(x^2 + 5 \bmod 3, 1 - 2x \bmod 3) = \gcd(x^2 - 1, 1 + x) = 1 + x$
$\gcd(x^2 + 5 \bmod 7, 1 - 2x \bmod 7) = \gcd(x^2 + 5, 3 + x) = 3 + x$

Factorization into prime ideals

For $a - b\theta$ in $\mathbb{Z}[\theta]$,

1. compute $n = \text{Norm}(a - b\theta)$
2. factor n in $\mathbb{Z}$
3. match each prime factor ℓ of n with a prime ideal:
   compute $\gcd(\underbrace{f(x) \bmod \ell}_{=(x+s)(x+t)}, a - bx \bmod \ell)$

$\theta = \sqrt{-5}$, $(a, b) = (1, 2)$, $a - b\theta = 1 - 2\sqrt{-5}$

$\text{Norm}(1 - 2\theta) = 1^2 + 5 \cdot 2^2 = 21 = 3 \cdot 7$
$\gcd(x^2 + 5 \bmod 3, 1 - 2x \bmod 3) = \gcd(x^2 - 1, 1 + x) = 1 + x$
$\gcd(x^2 + 5 \bmod 7, 1 - 2x \bmod 7) = \gcd(x^2 + 5, 3 + x) = 3 + x$

$$\underbrace{(1 - 2\theta)}_{\text{as an ideal}} = (3, 1 + x) \cdot (7, 3 + x)$$

Factorization into prime ideals

We now have **unique factorization** into prime ideals
$6 = (1+\sqrt{-5})(1-\sqrt{-5}) = 2 \cdot 3$

$$(1-\sqrt{-5}) = (1-\theta) = (2, x+1) \cdot (3, x-1)$$

$$(1+\sqrt{-5}) = (1+\theta) = (2, x+1) \cdot (3, x+1)$$

$p = 1109 = 33^2 + 5 \cdot 2^2$, $f = x^2 + 5$, $g = 2x - 33$

a, b	$2a - 33b$	$a^2 + 5b^2$	factor in $\mathbb{Z}[\theta]$
$-11, 1$	$-55 = -5 \cdot 11$	$126 = 2 \cdot 3^2 \cdot 7$	$(2, x+1)(3, x-1)^2(7, x-3)$
$-11, 8$	$-286 = -2 \cdot 11 \cdot 13$	$441 = 3^2 \cdot 7^2$	$(3, x+1)^2(7, x-3)^2$
$-3, 1$	$-39 = -3 \cdot 13$	$14 = 2 \cdot 7$	$(2, x+1)(7, x+3)$
$-1, 1$	$-35 = -5 \cdot 7$	$6 = 2 \cdot 3$	$(2, x+1)(3, x+1)$
$0, 1$	$-33 = -3 \cdot 11$	$5 = 5$	$(5, x)$
$1, 2$	$-64 = -2^6$	$21 = 3 \cdot 7$	$(3, x+1)(7, x+3)$
$1, 4$	$-130 = -2 \cdot 5 \cdot 13$	$81 = 3^4$	$(3, x-1)^4$
$3, 1$	$-27 = -3^3$	$14 = 2 \cdot 7$	$(2, x+1)(7, x-3)$
$4, 1$	$-25 = -5^2$	$21 = 3 \cdot 7$	$(3, x-1)(7, x+3)$
$5, 2$	$-56 = -2^3 \cdot 7$	$45 = 3^2 \cdot 5$	$(3, x-1)^2(5, x)$
$10, 1$	$-13 = -13$	$105 = 3 \cdot 5 \cdot 7$	$(3, x-1)(5, x)(7, x-3)$
$11, 1$	$-11 = -11$	$126 = 2 \cdot 3^2 \cdot 7$	$(2, x+1)(3, x+1)^2(7, x+3)$
$11, 8$	$-242 = -2 \cdot 11^2$	$441 = 3^2 \cdot 7^2$	$(3, x-1)^2(7, x+3)^2$

$p = 1109 = 33^2 + 5 \cdot 2^2,\ f = x^2 + 5,\ g = 2x - 33$

a, b	$2a - 33b$	$a^2 + 5b^2$	factor in $\mathbb{Z}[\theta]$
$-11, 1$	$-55 = -5 \cdot 11$	$126 = 2 \cdot 3^2 \cdot 7$	$(2, x+1)(3, x-1)^2(7, x-3)$
$-11, 8$	$-286 = -2 \cdot 11 \cdot 13$	$441 = 3^2 \cdot 7^2$	$(3, x+1)^2(7, x-3)^2$
$-3, 1$	$-39 = -3 \cdot 13$	$14 = 2 \cdot 7$	$(2, x+1)(7, x+3)$
$-1, 1$	$-35 = -5 \cdot 7$	$6 = 2 \cdot 3$	$(2, x+1)(3, x+1)$
$0, 1$	$-33 = -3 \cdot 11$	$5 = 5$	$(5, x)$
$1, 2$	$-64 = -2^6$	$21 = 3 \cdot 7$	$(3, x+1)(7, x+3)$
$1, 4$	$-130 = -2 \cdot 5 \cdot 13$	$81 = 3^4$	$(3, x-1)^4$
$3, 1$	$-27 = -3^3$	$14 = 2 \cdot 7$	$(2, x+1)(7, x-3)$
$4, 1$	$-25 = -5^2$	$21 = 3 \cdot 7$	$(3, x-1)(7, x+3)$
$5, 2$	$-56 = -2^3 \cdot 7$	$45 = 3^2 \cdot 5$	$(3, x-1)^2(5, x)$
$10, 1$	$-13 = -13$	$105 = 3 \cdot 5 \cdot 7$	$(3, x-1)(5, x)(7, x-3)$
$11, 1$	$-11 = -11$	$126 = 2 \cdot 3^2 \cdot 7$	$(2, x+1)(3, x+1)^2(7, x+3)$
$11, 8$	$-242 = -2 \cdot 11^2$	$441 = 3^2 \cdot 7^2$	$(3, x-1)^2(7, x+3)^2$

$p = 1109 = 33^2 + 5 \cdot 2^2,\ f = x^2 + 5,\ g = 2x - 33$

a, b	$2a - 33b$	$a^2 + 5b^2$	factor in $\mathbb{Z}[\theta]$
$-11, 1$	$-55 = -5 \cdot 11$	$126 = 2 \cdot 3^2 \cdot 7$	$(2, x+1)(3, x-1)^2(7, x-3)$
$-11, 8$	$-286 = -2 \cdot 11 \cdot 13$	$441 = 3^2 \cdot 7^2$	$(3, x+1)^2(7, x-3)^2$
$-3, 1$	$-39 = -3 \cdot 13$	$14 = 2 \cdot 7$	$(2, x+1)(7, x+3)$
$-1, 1$	$-35 = -5 \cdot 7$	$6 = 2 \cdot 3$	$(2, x+1)(3, x+1)$
$0, 1$	$-33 = -3 \cdot 11$	$5 = 5$	$(5, x)$
$1, 2$	$-64 = -2^6$	$21 = 3 \cdot 7$	$(3, x+1)(7, x+3)$
$1, 4$	$-130 = -2 \cdot 5 \cdot 13$	$81 = 3^4$	$(3, x-1)^4$
$3, 1$	$-27 = -3^3$	$14 = 2 \cdot 7$	$(2, x+1)(7, x-3)$
$4, 1$	$-25 = -5^2$	$21 = 3 \cdot 7$	$(3, x-1)(7, x+3)$
$5, 2$	$-56 = -2^3 \cdot 7$	$45 = 3^2 \cdot 5$	$(3, x-1)^2(5, x)$
$10, 1$	$-13 = -13$	$105 = 3 \cdot 5 \cdot 7$	$(3, x-1)(5, x)(7, x-3)$
$11, 1$	$-11 = -11$	$126 = 2 \cdot 3^2 \cdot 7$	$(2, x+1)(3, x+1)^2(7, x+3)$
$11, 8$	$-242 = -2 \cdot 11^2$	$441 = 3^2 \cdot 7^2$	$(3, x-1)^2(7, x+3)^2$

$$
\begin{array}{ccccccccccccc}
2 & 3 & 5 & 7 & 11 & 13 & \frac{1}{2} & (2, x+1) & (3, x+1) & (3, x-1) & (5, x) & (7, x+3) & (7, x-3)
\end{array}
$$

$$
M = \begin{bmatrix}
0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 2 & 0 & 0 & 1 \\
1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 2 & 0 & 0 & 0 & 2 \\
0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\
6 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\
1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 4 & 0 & 0 & 0 \\
0 & 3 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 2 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\
3 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 2 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\
0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 2 & 0 & 0 & 1 & 0 \\
1 & 0 & 0 & 0 & 2 & 0 & 1 & 0 & 0 & 2 & 0 & 2 & 0
\end{bmatrix}
$$

$$
\begin{array}{c}
\begin{array}{ccccccccccccc}
2 & 3 & 5 & 7 & 11 & 13 & \frac{1}{2} & (2, x+1) & (3, x+1) & (3, x-1) & (5, x) & (7, x+3) & (7, x-3)
\end{array}
\\
M = \begin{bmatrix}
 & & 1 & & 1 & & 1 & 1 & & 2 & & & 1 \\
1 & & & & 1 & 1 & 1 & & 2 & & & & 2 \\
 & 1 & & & & 1 & 1 & 1 & & & & 1 & \\
 & & 1 & 1 & & & 1 & 1 & 1 & & & & \\
 & 1 & & & 1 & & 1 & & & & 1 & & \\
6 & & & & & & 1 & & 1 & & & 1 & \\
1 & & 1 & & & 1 & 1 & & & 4 & & & \\
 & 3 & & & & & 1 & 1 & & & & & 1 \\
 & & 2 & & & & 1 & & & 1 & & 1 & \\
3 & & & 1 & & & 1 & & & 2 & 1 & & \\
 & & & & & 1 & 1 & & & 1 & 1 & & 1 \\
 & & & & 1 & & 1 & 1 & 2 & & & 1 & \\
1 & & & & 2 & & 1 & & & 2 & & 2 &
\end{bmatrix}
\end{array}
$$

$M =$

2	3	5	7	11	13	$\frac{1}{2}$	$(2, x+1)$	$(3, x+1)$	$(3, x-1)$	$(5, x)$	$(7, x+3)$	$(7, x-3)$
		1		1		1	−1		−2			−1
1				1	1	1		−2				−2
	1				1	1	−1				−1	
		1	1			1	−1	−1				
	1			1		1				−1		
6						1		−1			−1	
1		1			1	1			−4			
	3					1	−1					−1
		2				1			−1		−1	
3			1			1			−2	−1		
					1	1			−1	−1		−1
				1		1	−1	−2			−1	
1				2		1			−2		−2	

Example imaginary quadratic field

Right kernel $M \cdot \boldsymbol{x} = 0 \bmod (p-1)/4 = 277$:

$$\boldsymbol{x} = (\underbrace{1, 219, 40, 34, 79, 269}_{\text{rational side}}, \underbrace{276}_{1/2}, \underbrace{139, 211, 8, 20, 71, 240}_{\text{algebraic side}})$$

$\log 2 = 1$, $\log 1/2 = -1$

Rational side: logarithms of $\{2, 3, 5, 7, 11, 13\}$
$\rightarrow \log x_i / \log 2$
$\boldsymbol{x} = [1, 219, 40, 34, 79, 269] \bmod 277$
$\rightarrow$ order 4 subgroup
$\boldsymbol{v} = [1, 219, 594, 311, 910, 1100] \bmod p - 1$
Same logarithms as before.

Plan

Introduction

Index calculus algorithm

Coppersmith–Odlyzko–Schroeppel 1986

Factorization into prime ideals in quadratic number fields

Number Field Sieve with base-m

Number Field Sieve today: Joux–Lercier

Historical steps of NFS

Complexities:
Index calculus: $e^{(\sqrt{2}+o(1))\sqrt{(\log p)(\log\log p)}}$ Pomerance 87
Quadratic sieve: $e^{(1+o(1))\sqrt{(\log p)(\log\log p)}}$ (for factoring)
Lenstra–Pomerance 92

$\mathbb{Z}[i]$ generalized: Number Field and its ring of algebraic integers

Big improvement in the complexity:

$$L_p(\alpha, c) = e^{(c+o(1))(\log p)^{\alpha}(\log\log p)^{1-\alpha}}$$

Index calculus: $L_p(1/2, \sqrt{2})$
Quadratic sieve: $L_p(1/2, 1)$
Number Field Sieve: $L_p(1/3, c)$
Much faster for very large p (over around 100 digits)

Historical steps of NFS

Integer factorization:

- Lenstra, Lenstra, Manasse, Pollard: Special-NFS $L_N(1/3, c)$, $c = (32/9)^{1/3} = 1.526$, special integers $N = 2^n \pm 1$
- Buhler, HW Lenstra, Pomerance: NFS $L_N(1/3, c)$, $c = (64/9)^{1/3} = 1.923$
- Coppersmith: Multiple-NFS $L_N(1/3, 1.902)$

Applied to discrete logarithm computation:

- Gordon: NFS-DL in $L_p(1/3, c)$, $c = 3^{2/3} = 2.08$
- Schirokauer: NFS-DL in $L_p(1/3, c)$, $c = (64/9)^{1/3} = 1.923$

Setup: base-m technique

How to **reduce the size** of the numbers to factor?
Choose a degree $d > 2$ ($d \approx 3^{1/3}(\log p)^{1/3}/(\log\log p)^{1/3}$)
$m = \lfloor p^{1/d} \rceil$ a positive integer
Write p in base m: $p = f_0 + f_1 m + \ldots + f_{d-1} m^{d-1} + m^d$,
$0 \leq f_i < m$
Set $f = f_0 + f_1 x + \ldots + f_{d-1} x^{d-1} + x^d$
Set $g = x - m$

Morphisms

$f(x), g(x)$ irreducible in $\mathbb{Z}[x]$ s.t. $f(m) = g(m) = 0 \bmod p$
Let $\theta \in \mathbb{C}$ a root of f: $f(\theta) = 0$ in $\mathbb{C}$

Define a map from $\mathbb{Z}[\theta]$ to $\mathbb{Z}/p\mathbb{Z}$

$$\begin{array}{rcl} \phi\colon \mathbb{Z}[\theta] & \to & \mathbb{Z}/p\mathbb{Z} \\ \theta & \mapsto & m \bmod p \text{ where } m \in \mathbb{Z}/p\mathbb{Z},\ f(m) = 0 \bmod p \end{array}$$

ring homomorphism $\phi(a + b\theta) = a + bm$

$$\phi\ \underbrace{(a + b\theta)}_{\text{factor in } \mathbb{Z}[\theta]} = \underbrace{a + bm}_{\text{factor in } \mathbb{Z}} \quad \bmod p$$

Factorization of $a - b\theta$ in $\mathbb{Z}[\theta]$

1. Compute the algebraic norm in $\mathbb{Z}$:
$$\begin{aligned}\mathrm{Norm}(a-b\theta) &= b^d f(a/b)\\ &= f_0 b^d + f_1 a b^{d-1} + \ldots + f_{d-1} a^{d-1} b + a^d\end{aligned}$$
2. Factor $\mathrm{Norm}(a-b\theta)$ in $\mathbb{Z}$ into prime numbers
3. Deduce the factorization of $a - b\theta$ into prime ideals

Norm is multiplicative:

$$\begin{aligned}(a-b\theta) &= \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\cdots\mathfrak{p}_i^{e_i}\\ \mathrm{Norm}(a-b\theta) &= \mathrm{Norm}(\mathfrak{p}_1)^{e_1}\,\mathrm{Norm}(\mathfrak{p}_2)^{e_2}\cdots\mathrm{Norm}(\mathfrak{p}_i)^{e_i}\\ &= (p_1^{d_1})^{e_1}(p_2^{d_2})^{e_2}\cdots(p_i^{d_i})^{e_i}\end{aligned}$$

The $\mathfrak{p}_i$ are prime ideals

Prime ideals $\mathfrak{p}_i$ in a number field

$\mathfrak{p}_i$ is a prime ideal and is generated by two elements:

- a prime number p_i s.t. $\mathfrak{p}_i$ has norm $p_i^{d_i}$
- an irreducible factor of f mod p_i of degree d_i

Magma: `Generators(I)`, `TwoGenerator(I)`
SageMath:`I.gens(), I.gens_reduced()`
In $\mathbb{Z}[i]$: we had $(2, x+1), (3, x+2), (3, x-2)$...
Not every prime ideal $\mathfrak{p}_i$ has one generator, however,

Class number

The *Class number* h_K of a number field K is an integer such that any $\mathfrak{p}_i^{h_K}$ is principal ($\exists$ a generator g_i of $\mathfrak{p}_i^{h_K}$).

If $h_K = 1$, then any ideal is principal ($\exists$ a generator).

Example base-m

$p = 1109$
$d = 3,\ m = \lfloor p^{1/3} \rceil = 10$
$1109 = 10^3 + 10^2 + 9 \to f = x^3 + x^2 + 9,\ g = x - 10$

$\text{Res}(f, g) = -1109 = -p$
$\gcd(f \bmod p, g \bmod p) = x - 10$
$f(10) = g(10) = 0 \bmod p$

Define the map

$$\begin{array}{rcl} \phi_f : \mathbb{Z}[\theta] & \to & \mathbb{Z}/p\mathbb{Z} \\ \theta & \mapsto & m \bmod p \text{ where } m = 10,\ f(m) = 0 \bmod p \end{array}$$

ϕ_f is a ring homomorphism
$\phi_f(a + b\theta) = a + bm$

Example base-m: ideal factorization

Factor $f(x)$ mod ℓ for each $\ell \in \{2, 3, 5, 7, 11, 13\}$

ℓ	$f(x)$ mod ℓ
2	$x^3 + x^2 + 1$
3	$(x+1)x^2$
5	$(x+2)(x^2+4x+2)$
7	$(x+5)(x^2+3x+6)$
11	$(x+10)(x^2+2x+2)$
13	$(x+4)(x+5)^2$
$\vdots$	
71	$(x+9)(x+17)(x+46)$
73	$(x+37)(x^2+37x+18)$
79	$(x+33)(x^2+47x+29)$
83	$(x+62)(x^2+22x+47)$
89	$(x+21)(x+73)(x+85)$
97	$x^3 + x^2 + 9$

Example base-m: ideal factorization

Factor $f(x)$ mod ℓ for each $\ell \in \{2, 3, 5, 7, 11, 13\}$

Keep only the degree 1 factors

$\rightarrow$ correspond to degree 1 prime ideals

ℓ	$f(x)$ mod ℓ
2	$x^3 + x^2 + 1$
3	$(x+1)x^2$
5	$(x+2)(x^2+4x+2)$
7	$(x+5)(x^2+3x+6)$
11	$(x+10)(x^2+2x+2)$
13	$(x+4)(x+5)^2$
$\vdots$	
71	$(x+9)(x+17)(x+46)$
73	$(x+37)(x^2+37x+18)$
79	$(x+33)(x^2+47x+29)$
83	$(x+62)(x^2+22x+47)$
89	$(x+21)(x+73)(x+85)$
97	$x^3 + x^2 + 9$

Example base-m: ideal factorization

Factor $f(x)$ mod ℓ for each $\ell \in \{2, 3, 5, 7, 11, 13\}$

Keep only the degree 1 factors

$\rightarrow$ correspond to degree 1 prime ideals

ℓ	$f(x)$ mod ℓ
2	
3	$(x+1)x^2$
5	$(x+2)$
7	$(x+5)$
11	$(x+10)$
13	$(x+4)(x+5)^2$

Example base-m: ideal factorization

Factor $f(x)$ mod ℓ for each $\ell \in \{2, 3, 5, 7, 11, 13\}$

Keep only the degree 1 factors

$\rightarrow$ correspond to degree 1 prime ideals

ℓ	$f(x)$ mod ℓ	generator
2		
3	$(x+1)x^2$	$(\theta^2+\theta)/3, \theta$
5	$(x+2)$	$2+\theta$
7	$(x+5)$	$(2\theta-\theta^2)/3$
11	$(x+10)$	$-1+\theta$
13	$(x+4)(x+5)^2$	$(4\theta+\theta^2)/3, 2+(\theta+\theta^2)/3$

Example base-m: ideal factorization and unit

Fondamental unit $u_f = \alpha_f(\alpha_f + 1)/3 - 1$
Need to compute $\log u_f$
Add a column for u_f in the matrix

Example base-m: ideal factorization and unit

Fondamental unit $u_f = \alpha_f(\alpha_f + 1)/3 - 1$
Need to compute $\log u_f$
Add a column for u_f in the matrix

But then we need unique factorization of elements
We need one generator for each prime ideal

Example base-m: ideal factorization and unit

Fondamental unit $u_f = \alpha_f(\alpha_f + 1)/3 - 1$
Need to compute $\log u_f$
Add a column for u_f in the matrix

But then we need unique factorization of elements
We need one generator for each prime ideal

1. compute one generator $g_i \in \mathbb{Z}[\theta]$ per prime ideal $(\ell_i, x + r_i)$
   possible only if the ideal is principal
2. write ideal $(a - b\theta) = \prod_i \underbrace{(\ell_i, x + r_i)}_{\text{generator } g_i}^{e_i}$ as before
3. compute $\prod_i g_i^{e_i}$ product of elements in $\mathbb{Z}[\theta]$
4. $\exists$ u_i unit s.t. $a - b\theta = \prod_i g_i^{e_i} \cdot u_i$
   $u_i = (a - b\theta)/(\prod_i g_i^{e_i})$ as elements in $\mathbb{Z}[\theta]$
5. compute exponent e_{u_i} s.t. $u_i = u_f^{e_{u_i}}$
6. $a - b\theta = \prod_i g_i^{e_i} \cdot u_f^{e_{u_i}}$

Example base-m

a, b	$a - bm$	$9b^3 + a^2b + a^3$	factor in $\mathbb{Z}[\theta]$	unit
$-10, 1$	$-20 = -2^2 \cdot 5$	$-891 = -3^4 \cdot 11$	$(3, x+1)^4(11, x+10)$	1
$-6, 5$	$-56 = -2^3 \cdot 7$	$1089 = 3^2 \cdot 11^2$	$(3, x^2)(11, x+10)^2$	$-u_f$
$-5, 1$	$-15 = -3 \cdot 5$	$-91 = -7 \cdot 13$	$(7, x+5)(13, x+5)$	u_f
$-5, 2$	$-25 = -5^2$	$-3 = -3$	$(3, x+1)$	$-u_f^2$
$-4, 1$	$-14 = -2 \cdot 7$	$-39 = -3 \cdot 13$	$(3, x+1)(13, x+4)$	1
$-3, 1$	$-13 = -13$	$-9 = -3^2$	$(3, x^2)$	u_f
$-2, 1$	$-12 = -2^2 \cdot 3$	$5 = 5$	$(5, x+2)$	$-u_f$
$-1, 1$	$-11 = -11$	$9 = 3^2$	$(3, x+1)^2$	1
$0, 1$	$-10 = -2 \cdot 5$	$9 = 3^2$	$(3, x^2)$	-1
$1, 1$	$-9 = -3^2$	$11 = 11$	$(11, x+10)$	-1
$2, 1$	$-8 = -2^3$	$21 = 3 \cdot 7$	$(3, x+1)(7, x+5)$	-1
$3, 1$	$-7 = -7$	$45 = 3^2 \cdot 5$	$(3, x^2)(5, x+2)$	1
$6, 5$	$-44 = -2^2 \cdot 11$	$1521 = 3^2 \cdot 13^2$	$(3, x^2)(13, x+4)^2$	$-u_f^{-1}$
$8, 1$	$-2 = -2$	$585 = 3^2 \cdot 5 \cdot 13$	$(3, x+1)^2(5, x+2)(13, x+5)$	-1
$9, 1$	$-1 = -1$	$819 = 3^2 \cdot 7 \cdot 13$	$(3, x^2)(7, x+5)(13, x+4)$	-1

$$
\begin{array}{c}
\begin{array}{cccccccccccccc}
2 & 3 & 5 & 7 & 11 & 13 & u_f & (3,x+1) & (3,x^2) & (5,x+2) & (7,x-2) & (11,x-1) & (13,x+4) & (13,x+5)
\end{array}
\\
M = \begin{bmatrix}
2 & 0 & 1 & 0 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 1 & 0 & 0 \\
3 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 2 & 0 & 0 \\
0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\
0 & 0 & 2 & 0 & 0 & 0 & 2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
2 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
3 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\
2 & 0 & 0 & 0 & 1 & 0 & -1 & 0 & 1 & 0 & 0 & 0 & 2 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 1 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0
\end{bmatrix}
\end{array}
$$

$M =$

2	3	5	7	11	13	u_f	$(3, x+1)$	$(3, x^2)$	$(5, x+2)$	$(7, x-2)$	$(11, x-1)$	$(13, x+4)$	$(13, x+5)$
2		1					4				1		
3			1			1		1			2		
	1	1				1				1			1
		2				2	1						
1			1				1					1	
					1	1		1					
2	1					1			1				
				1			2						
1		1						1					
	2										1		
3							1			1			
			1					1	1				
2				1		-1		1				2	
1							2		1				1
								1		1		1	

$M =$

	2	3	5	7	11	13	u_f	$(3, x+1)$	$(3, x^2)$	$(5, x+2)$	$(7, x-2)$	$(11, x-1)$	$(13, x+4)$	$(13, x+5)$
	2		1					−4				−1		
	3			1			−1		−1			−2		
		1	1				−1				−1			−1
			2				−2	−1						
	1			1				−1					−1	
						1	−1		−1					
	2	1					−1			−1				
					1			−2						
	1		1						−1					
		2										−1		
	3							−1			−1			
				1					−1	−1				
	2				1		1		−1				−2	
	1							−2		−1				−1
									−1		−1		−1	

Example base-m

Right kernel $M \cdot \boldsymbol{x} = 0 \bmod (p-1)/4 = 277$:

$$\boldsymbol{x} = (\underbrace{1, 219, 40, 34, 79, 269}_{\text{rational side}}, \underbrace{228}_{\text{unit}}, \underbrace{178, 41, 270, 102, 161, 134, 206}_{\text{algebraic side}})$$

Rational side: logarithms of $\{2, 3, 5, 7, 11, 13\}$
$\rightarrow \log x_i / \log 2$
$\boldsymbol{x} = [1, 219, 40, 34, 79, 269] \bmod 277$
$\rightarrow$ order 4 subgroup
$\boldsymbol{v} = [1, 219, 594, 311, 910, 1100] \bmod p - 1$
Same logarithms as before.

Relation collection: sizes of integers to factor

- small integers a, b in $[-A, A]$, $A \approx e^{((8/9)^{1/3}+o(1))(\log p)^{1/3}(\log\log p)^{2/3}}$
- factor $a - b\theta$ in $\mathbb{Z}[\theta]$
- factor $a - bm$ in $\mathbb{Z}$

$|\operatorname{Norm}(a - b\theta)| \leq d\ m \max(|a|, |b|)^d \approx d\ p^{1/d} A^d$
$|a - bm| \leq 2Am \approx 2Ap^{1/d}$

integer to factor	quadratic	base-m
$\operatorname{Norm}(a - b\theta)$	A^2	$d\ p^{1/d} A^d$
$aV - bU$	$A\sqrt{p}$	
$a - bm$		$Ap^{1/d}$
A	$L_p(1/2, 1/\sqrt{2})$	$L_p(1/3, (8/9)^{1/3})$
A^2	$L_p(1/2, \sqrt{2})$	$L_p(1/3, (64/9)^{1/3})$

Weber Denny Zayer record computations in $\mathbb{F}_p$

https://listserv.nodak.edu/cgi-bin/wa.exe?A2=NMBRTHRY;40d1ce60.9604

Date: Tue, 9 Apr 1996 09:04:20 EDT

$$p = 31081938120519680804196114121911010119642610196603091971180519412712199932 7$$

75 dd, 248 bits

$$f = 41440163x^4 + 8899586579547x^3 + 50013054105621x^2 - 385158712921327x - 226856042090363$$

$$g = x - 41988177346362907 44 = x - m$$

$$f(m) = g(m) = 0 \bmod p$$

Sieving region: $a \in]-10^7, 10^7[$, $b \in [1, 1.2 \cdot 10^6[$

Area: $2.4 \cdot 10^{13} = 2^{44.448}$

Smoothness bounds:

Rational g-side: $B_r = 48593$, $\#\mathcal{F}_r = 5000$

Algebraic f-side: $B_a = 224737$, $\#\mathcal{F}_a = 20058$

SageMath experimentation

Task:
run the Sage code with $p = 1109$ and $f = x^3 + x^2 + x - 1$.

Plan

Introduction

Index calculus algorithm

Coppersmith–Odlyzko–Schroeppel 1986

Factorization into prime ideals in quadratic number fields

Number Field Sieve with base-m

Number Field Sieve today: Joux–Lercier

- Rational reconstruction and lattice reduction
- Joux–Lercier polynomial selection method
- Example with monic f, g, principal K_f, K_g

Half extended Euclidean algorithm

Goal

Given $y \in \mathbb{Z}/p\mathbb{Z}$, compute $u, v \in \mathbb{Z}$, $|u|, |v| \approx \sqrt{p}$, s.t. $u/v \equiv y \bmod p$

`xgcd(y,p)` gives w, v s.t. $wp + vy = \gcd(y, p)$ $(= 1)$.
Idea: stop at $w_i p + v_i y = u_i$ s.t. $|v_i|, |u_i| \approx \sqrt{p}$
Then $v_i y \equiv u_i \bmod p \Leftrightarrow y \equiv u_i/v_i \bmod p$ and u_i, v_i are of balanced size, and much smaller than y.

Lattice basis reduction

Goal

Given $y \in \mathbb{Z}/p\mathbb{Z}$, compute $u, v \in \mathbb{Z}$, $|u|, |v| \approx \sqrt{p}$,
s.t. $u/v \equiv y \bmod p$

Rewrite as a lattice basis:
Given $\{\boldsymbol{b}_1 = (p, 0), \boldsymbol{b}_2 = (y, 1)\}$, compute a short basis $\{\boldsymbol{b}'_1 = (u, v), \boldsymbol{b}'_2 = (u_1, v_1)\}$ s.t. the (Euclidean) norms of $\boldsymbol{b}'_i$ are as small as possible: successive minima.
$\exists(\lambda, \mu)$ s.t. $\boldsymbol{b}'_1 = \lambda \boldsymbol{b}_1 + \mu \boldsymbol{b}_2$
that is $u = \lambda p + \mu y$, and $v = \mu$
$\Leftrightarrow u \equiv vy \bmod p \Leftrightarrow y \equiv u/v \bmod p$

Lagrange–Gauss lattice basis reduction

input: basis $\{\boldsymbol{b}_1, \boldsymbol{b}_2\}$, $\boldsymbol{b}_i \in \mathbb{Z}^2$ of a 2-dim lattice L
output: Lagrange-Gauss reduced basis of L

$\mu = \boldsymbol{b}_1 \cdot \boldsymbol{b}_2 / \|\boldsymbol{b}_1\|^2$ # *scalar product, Euclidean norm*
$\boldsymbol{b}_2 = \boldsymbol{b}_2 - \lfloor \mu \rceil \boldsymbol{b}_1$ # *reduce norm*
while $\|\boldsymbol{b}_2\|^2 < \|\boldsymbol{b}_1\|^2$ **do**
    $(\boldsymbol{b}_1, \boldsymbol{b}_2) = (\boldsymbol{b}_2, -\boldsymbol{b}_1)$ # *swap*
    $\mu = \boldsymbol{b}_1 \cdot \boldsymbol{b}_2 / \|\boldsymbol{b}_1\|^2$
    $\boldsymbol{b}_2 = \boldsymbol{b}_2 - \lfloor \mu \rceil \boldsymbol{b}_1$ # *reduce norm*
return $(\boldsymbol{b}_1, \boldsymbol{b}_2)$

Properties

$\|\boldsymbol{b}_1\| \leq \|\boldsymbol{b}_2\|$ and $|\langle \boldsymbol{b}_1, \boldsymbol{b}_2 \rangle| \leq \|\boldsymbol{b}_1\|^2/2$
$\|\boldsymbol{b}_1\| \leq (4/3)^{1/4} \operatorname{vol}(L(\{\boldsymbol{b}_1, \boldsymbol{b}_2\}))^{1/2}$

LLL lattice reduction

- Lenstra, Lenstra, Lovász
- For higher dimension lattices
- optimal for the Euclidean norm
- see e.g. Nguyen–Vallée handbook on LLL
- dedicated optimized software (`fplll`, etc)

Properties of LLL

An LLL-reduced basis $\{\boldsymbol{b}_i\}_{1 \le i \le n}$ of a lattice L of dimension d, with factor (η, δ) such that $1/4 < \delta < 1$ and $1/2 < \eta < \sqrt{\delta}$, satisfies:

$$\|\boldsymbol{b}_1\| \le (\delta - \eta^2)^{(d-1)/4} \mathrm{vol}(L)^{1/d}$$

where $\mathrm{vol}(L) = \sqrt{\det(\boldsymbol{B}\boldsymbol{B}^T)}$ and $\boldsymbol{B}$ is any basis of L

Joux–Lercier polynomial selection (2003)

Reduce even more the size of norms
2 algebraic sides: irreducible polynomials f, g in $\mathbb{Z}[x]$
We need that f, g share one common root m mod p

Choose $\deg f = d$, then $\deg g = d - 1$

Joux–Lercier polynomial selection (2003)

Reduce even more the size of norms
2 algebraic sides: irreducible polynomials f, g in $\mathbb{Z}[x]$
We need that f, g share one common root m mod p

Choose $\deg f = d$, then $\deg g = d - 1$

1. choose f of degree d, tiny coefficients, irreducible over $\mathbb{Q}$, with a root r_0 mod p: $x - r_0$ is a factor of f mod p
   We want $g(r_0) = 0$ mod p, i.e. $x - r_0$ is a factor of g mod p
2. Define the vector subspace in $\mathbb{Z}[x]$ of all the polynomials multiple of p and $x - r_0$ and degree up to $d - 1$:
   $\{p, x - r_0, x(x - r_0), x^2(x - r_0), \ldots, x^{d-2}(x - r_0)\}$
3. Write in canonical basis $\{1, x, x^2, \ldots\}$:
   it defines a lattice
   each row $1 \leqslant i < d$ corresponds to $x^{i-1}(x - r_0)$
4. Reduce the lattice over $\mathbb{Z}$: get a short vector
   $\rightarrow$ polynomial with small coefficients

Joux–Lercier polynomial selection (2003)

$$M = \begin{bmatrix} p & 0 & \cdots & 0 \\ -r_0 & 1 & 0 & \vdots \\ 0 & \ddots & \ddots & 0 \\ 0 & 0 & -r_0 & 1 \end{bmatrix} \begin{matrix} \}\text{1 row} \\ \left.\begin{matrix} \\ \\ \end{matrix}\right\} d-1 \text{ rows} \end{matrix} \rightarrow \mathrm{LLL}(M) = \begin{bmatrix} g_0 & g_1 & \cdots & g_{d-1} \\ & & & \\ & & * & \\ & & & \end{bmatrix}$$

a short vector is a linear combination of $x^i(x - r_0)$ and p:
has the root r_0 mod p

$g = g_0 + g_1 x + \cdots + g_{d-1}x^{d-1}$, $||g||_\infty = O(p^{1/d})$ and
$g(r_0) = 0 \bmod p$

Example: Joux–Lercier, polynomial selection

$p = 1109$
$f = x^3 - x + 1$ monic and irreducible over $\mathbb{Q}$
$f = (x + 347)(x^2 + 762x + 636) \bmod p$

$$M = \begin{bmatrix} 1109 & 0 & 0 \\ 347 & 1 & 0 \\ 0 & 347 & 1 \end{bmatrix} \begin{matrix} p \\ 347 + x \\ 347x + x^2 \end{matrix} \rightarrow \text{LLL} \rightarrow \begin{bmatrix} 6 & 6 & 5 \\ 1 & 10 & -5 \\ -11 & 5 & 1 \end{bmatrix}$$

$g = 6 + 6x + 5x^2$ irreducible
$g = -1 - 10x - 5x^2$ irreducible
$g = \mathbf{-11 + 5x + x^2}$ irreducible and monic

$\mathrm{Res}(f, g) = -1109 = -p$
$\gcd(f \bmod p, g \bmod p) = x + 347$
Common root $m = -347 \bmod p$
$f(-347) = g(-347) = 0 \bmod p$

Example Joux–Lercier: maps

f-side: $f = x^3 - x + 1$, α_f root of f in $\mathbb{C}$
g-side: $g = x^2 + 5x - 11$, α_g root of g in $\mathbb{C}$

Define two maps

$$\begin{array}{rcl} \phi_f : \mathbb{Z}[\alpha_f] & \to & \mathbb{Z}/p\mathbb{Z} \\ \alpha_f & \mapsto & m \bmod p \text{ where } m = -347,\ f(m) = 0 \bmod p \end{array}$$

$$\begin{array}{rcl} \phi_g : \mathbb{Z}[\alpha_g] & \to & \mathbb{Z}/p\mathbb{Z} \\ \alpha_g & \mapsto & m \bmod p \text{ where } m = -347,\ g(m) = 0 \bmod p \end{array}$$

ϕ_f, ϕ_g are ring homomorphisms
$\phi_f(a + b\alpha_f) = a + bm$
$\phi_g(a + b\alpha_g) = a + bm$

Example Joux–Lercier, factor basis $\mathcal{F}_f, \mathcal{F}_g$

f-side: collect relations $(a - b\alpha_f) = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\cdots\mathfrak{p}_B^{e_B}$
g-side: collect relations $(a - b\alpha_g) = \mathfrak{q}_1^{e_1}\mathfrak{q}_2^{e_2}\cdots\mathfrak{q}_B^{e_B}$
Where $\mathfrak{p}_i$, $\mathfrak{q}_j$ are *prime ideals*
The set of $\mathfrak{p}_i$, $\mathfrak{q}_j$ is called the *factor basis*

Relations:

$$\phi_f(a - b\alpha_f) = a - bm = \phi_g(a - b\alpha_g)$$

$$\phi_f(a - b\alpha_f) = \phi_f(\mathfrak{p}_1^{e_1})\cdots\phi_f(\mathfrak{p}_B^{e_B}) = a - bm$$

$$\phi_g(a - b\alpha_g) = \phi_g(\mathfrak{q}_1^{e_1})\cdots\phi_g(\mathfrak{q}_B^{e_B}) = a - bm$$

Example Joux–Lercier: f-side factor basis $\mathcal{F}_f$

$f(x) = x^3 - x + 1$, looking for the *prime ideals* $\mathfrak{p}$ of K_f

ℓ	$f(x) \bmod \ell$
2	$x^3 + x + 1$
3	$x^3 + 2x + 1$
5	$(x+2)(x^2+3x+3)$
7	$(x+5)(x^2+2x+3)$
11	$(x+6)(x^2+5x+2)$
13	$x^3 + 12x + 1$
17	$(x+5)(x^2+12x+7)$
19	$(x+6)(x^2+13x+16)$
23	$(x+3)(x+10)^2$

Example Joux–Lercier: f-side factor basis $\mathcal{F}_f$

$f(x) = x^3 - x + 1$, looking for the *prime ideals* $\mathfrak{p}$ of K_f

ℓ	$f(x) \bmod \ell$
5	$(x+2)$
7	$(x+5)$
11	$(x+6)$
17	$(x+5)$
19	$(x+6)$
23	$(x+3)(x+10)^2$

Example Joux–Lercier: f-side factor basis $\mathcal{F}_f$

$f(x) = x^3 - x + 1$, looking for the *prime ideals* $\mathfrak{p}$ of K_f

ℓ	$f(x) \bmod \ell$
5	$(x+2)$
7	$(x+5)$
11	$(x+6)$
17	$(x+5)$
19	$(x+6)$
23	$(x+3)(x+10)^2$

Keep only the degree 1 factors
$\rightarrow$ correspond to degree 1 prime ideals

Example Joux–Lercier: f-side factor basis $\mathcal{F}_f$

$f(x) = x^3 - x + 1$, looking for the *prime ideals* $\mathfrak{p}$ of K_f

ℓ	$f(x)$ mod ℓ	$\mathfrak{p}$ generator
5	$(x+2)$	$\alpha_f + 2$
7	$(x+5)$	$\alpha_f - 2$
11	$(x+6)$	$2\alpha_f + 1$
17	$(x+5)$	$3\alpha_f - 2$
19	$(x+6)$	$3\alpha_f - 1$
23	$(x+3)(x+10)^2$	$\alpha_f + 3,\ 2\alpha_f - 3$

Keep only the degree 1 factors
$\rightarrow$ correspond to degree 1 prime ideals

Example Joux–Lercier: g-side factor basis $\mathcal{F}_g$

$g(x) = x^2 + 5x - 11$, looking for the *prime ideals* $\mathfrak{q}$ of K_g

ℓ	$g(x) \bmod \ell$
2	$x^2 + x + 1$
3	$(x+1)^2$
5	$(x+1)(x+4)$
7	$x^2 + 5x + 3$
11	$x(x+5)$
13	$(x+8)(x+10)$
17	$(x+2)(x+3)$
19	$x^2 + 5x + 8$
23	$(x+14)^2$

Example Joux–Lercier: g-side factor basis $\mathcal{F}_g$

$g(x) = x^2 + 5x - 11$, looking for the *prime ideals* $\mathfrak{q}$ of K_g

ℓ	$g(x) \bmod \ell$
3	$(x+1)^2$
5	$(x+1)(x+4)$
11	$x(x+5)$
13	$(x+8)(x+10)$
17	$(x+2)(x+3)$
23	$(x+14)^2$

Example Joux–Lercier: g-side factor basis $\mathcal{F}_g$

$g(x) = x^2 + 5x - 11$, looking for the *prime ideals* $\mathfrak{q}$ of K_g

ℓ	$g(x) \bmod \ell$
3	$(x+1)^2$
5	$(x+1)(x+4)$
11	$x(x+5)$
13	$(x+8)(x+10)$
17	$(x+2)(x+3)$
23	$(x+14)^2$

Keep only the degree 1 factors
$\rightarrow$ correspond to degree 1 prime ideals

Example Joux–Lercier: g-side factor basis $\mathcal{F}_g$

$g(x) = x^2 + 5x - 11$, looking for the *prime ideals* $\mathfrak{q}$ of K_g

ℓ	$g(x) \bmod \ell$	$\mathfrak{q}$ generator
3	$(x+1)^2$	$\alpha_g + 7$
5	$(x+1)(x+4)$	$\alpha_g + 6,\ \alpha_g - 1$
11	$x(x+5)$	$\alpha_g,\ \alpha_g + 5$
13	$(x+8)(x+10)$	$\alpha_g + 8,\ \alpha_g - 3$
17	$(x+2)(x+3)$	$\alpha_g + 2,\ \alpha_g + 3$
23	$(x+14)^2$	$-3\alpha_g + 4$

Keep only the degree 1 factors
$\rightarrow$ correspond to degree 1 prime ideals

Example Joux–Lercier: factor basis $\mathcal{F}_f$, $\mathcal{F}_g$

$$\begin{aligned}
\mathcal{F}_f = &\{(5, x+2), (7, x+5), (11, x+6), (17, x+5),\\
&(19, x+6), (23, x+3), (23, x+10))\}\\
\mathcal{U}_f &= \langle -1, \alpha_f \rangle
\end{aligned}$$

K_f is principal: generators (the norm is in subscript)

$$\begin{aligned}
\mathcal{F}_f = &\{\alpha_f + 2_{(5)}, \alpha_f - 2_{(7)}, 2\alpha_f + 1_{(11)}, 3\alpha_f - 2_{(17)},\\
&3\alpha_f - 1_{(19)}, \alpha_f + 3_{(23)}, 2\alpha_f - 3_{(23)}\}
\end{aligned}$$

$$\begin{aligned}
\mathcal{F}_g = &\{(3, x+1), (5, x+1), (5, x+4), (11, x), (11, x+5),\\
&(13, x+8), (13, x+10), (17, x+2), (17, x+3), (23, x+14)\}\\
\mathcal{U}_g &= \langle -1, 3\alpha_g - 5 \rangle
\end{aligned}$$

K_g is principal: generators

$$\begin{aligned}
\mathcal{F}_g = &\{\alpha_g + 7_{(3)}, \alpha_g + 6_{(5)}, \alpha_g - 1_{(5)}, {\alpha_g}_{(11)}, \alpha_g + 5_{(11)},\\
&\alpha_g + 8_{(13)}, \alpha_g - 3_{(13)}, \alpha_g + 2_{(17)}, \alpha_g + 3_{(17)}, -3\alpha_g + 4_{(23)}\}
\end{aligned}$$

Example Joux–Lercier: Norm and Resultant

$f = x^3 - x + 1$
$g = x^2 + 5x - 11$

f, g are monic

$\text{Norm}(a - b\alpha_f) = \text{Res}(a - bx, f(x)) = a^3 - ab^2 + b^3$
$\text{Norm}(a - b\alpha_g) = \text{Res}(a - bx, g(x)) = a^2 + 5ab - 11b^2$

- Factor the integer $a^3 - ab^2 + b^3$
- Factor the integer $a^2 + 5ab - 11b^2$

Store the (a, b) pairs s.t. both integers are smooth

Example Joux–Lercier, $f = x^3 - x + 1$, $g = x^2 + 5x - 11$

$$A = 11,\ B_f = B_g = 23,\ u_f = \alpha_f,\ u_g = 3\alpha_g - 5$$

a, b	$a^3 - ab^2 + b^3$	factor in $\mathbb{Z}[\alpha_f]$	unit	$a^2 + 5ab - 11b^2$	factor in $\mathbb{Z}[\alpha_g]$	unit
$-11, 5$	$-931 = -7^2 \cdot 19$	$(7, x+5)^2(19, x+6)$	$-u_f{}^{-9}$	$-429 = -3 \cdot 11 \cdot 13$	$(3, x+1)(11, x)(13, x+10)$	1
$-11, 9$	$289 = 17^2$	$(17, x+5)^2$	$-u_f{}^{-13}$	$-1265 = -5 \cdot 11 \cdot 23$	$(5, x+4)(11, x)(23, x+14)$	$-u_g{}^{-1}$
$-6, 1$	$-209 = -11 \cdot 19$	$(11, x+6)(19, x+6)$	$-u_f{}^{-2}$	$-5 = -5$	$(5, x+1)$	-1
$-5, 1$	$-119 = -7 \cdot 17$	$(7, x+5)(17, x+5)$	$-u_f{}^{-6}$	$-11 = -11$	$(11, x+5)$	-1
$-4, 3$	$-1 = -1$		$u_f{}^{-13}$	$-143 = -11 \cdot 13$	$(11, x+5)(13, x+10)$	1
$-4, 7$	$475 = 5^2 \cdot 19$	$(5, x+2)^2(19, x+6)$	$u_f{}^3$	$-663 = -3 \cdot 13 \cdot 17$	$(3, x+1)(13, x+8)(17, x+3)$	u_g
$-3, 1$	$-23 = -23$	$(23, x+3)$	-1	$-17 = -17$	$(17, x+3)$	-1
$-3, 2$	$-7 = -7$	$(7, x+5)$	$u_f{}^{-8}$	$-65 = -5 \cdot 13$	$(5, x+4)(13, x+8)$	-1
$-2, 1$	$-5 = -5$	$(5, x+2)$	-1	$-17 = -17$	$(17, x+2)$	-1
$-1, 1$	$1 = 1$		$u_f{}^{-4}$	$-15 = -3 \cdot 5$	$(3, x+1)(5, x+1)$	u_g
$0, 1$	$1 = 1$		$-u_f$	$-11 = -11$	$(11, x)$	-1
$1, 1$	$1 = 1$		$-u_f{}^3$	$-5 = -5$	$(5, x+4)$	-1
$1, 2$	$5 = 5$	$(5, x+2)$	$u_f{}^6$	$-33 = -3 \cdot 11$	$(3, x+1)(11, x+5)$	u_g
$2, 1$	$7 = 7$	$(7, x+5)$	-1	$3 = 3$	$(3, x+1)$	$-u_g$
$2, 3$	$17 = 17$	$(17, x+5)$	-1	$-65 = -5 \cdot 13$	$(5, x+1)(13, x+8)$	u_g
$3, 1$	$25 = 5^2$	$(5, x+2)^2$	$u_f{}^8$	$13 = 13$	$(13, x+10)$	-1
$3, 2$	$23 = 23$	$(23, x+10)$	-1	$-5 = -5$	$(5, x+1)$	u_g
$4, 3$	$55 = 5 \cdot 11$	$(5, x+2)(11, x+6)$	$u_f{}^7$	$-23 = -23$	$(23, x+14)$	1
$5, 1$	$121 = 11^2$	$(11, x+6)^2$	$-u_f{}^3$	$39 = 3 \cdot 13$	$(3, x+1)(13, x+8)$	$-u_g$
$5, 6$	$161 = 7 \cdot 23$	$(7, x+5)(23, x+3)$	$u_f{}^3$	$-221 = -13 \cdot 17$	$(13, x+10)(17, x+2)$	1
$7, 2$	$323 = 17 \cdot 19$	$(17, x+5)(19, x+6)$	$u_f{}^{-4}$	$75 = 3 \cdot 5^2$	$(3, x+1)(5, x+4)^2$	1
$8, 5$	$437 = 19 \cdot 23$	$(19, x+6)(23, x+3)$	$-u_f{}^2$	$-11 = -11$	$(11, x+5)$	u_g

Example Joux–Lercier: Matrix

Build the matrix of relations:

- one row per (a, b) pair s.t. both norms are smooth
- one column per prime ideal
- one column per unit ($u_f = \alpha_f$, $u_g = 3\alpha_g - 5$)
- store the exponents

α_f (1)	α_f+2 (5)	α_f-2 (7)	$2\alpha_f+1$ (11)	$3\alpha_f-2$ (17)	$3\alpha_f-1$ (19)	α_f+3 (23)	$2\alpha_f-3$ (23)	$\alpha_g+7(3)$	$\alpha_g+6(5)$	$\alpha_g-1(5)$	$\alpha_g(11)$	$\alpha_g+5(11)$	$\alpha_g+8(13)$	$\alpha_g-3(13)$	$\alpha_g+2(17)$	$\alpha_g+3(17)$	$-3\alpha_g+4(23)$	$3\alpha_g-5(1)$
−9	0	2	0	0	1	0	0	1	0	0	1	0	0	1	0	0	0	0
−13	0	0	0	2	0	0	0	0	0	1	1	0	0	0	0	0	1	−1
−2	0	0	1	0	1	0	0	0	1	0	0	0	0	0	0	0	0	0
−6	0	1	0	1	0	0	0	0	0	0	0	1	0	0	0	0	0	0
−13	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0
3	2	0	0	0	1	0	0	1	0	0	0	0	1	0	0	1	0	1
0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	1	0	0
−8	0	1	0	0	0	0	0	0	0	1	0	0	1	0	0	0	0	0
0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0
−4	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	1
1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0
6	1	0	0	0	0	0	0	1	0	0	0	1	0	0	0	0	0	1
0	0	1	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	1
0	0	0	0	1	0	0	0	0	1	0	0	0	1	0	0	0	0	1
8	2	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0
0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	1
7	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0
3	0	0	2	0	0	0	0	1	0	0	0	0	1	0	0	0	0	1
3	0	1	0	0	0	1	0	0	0	0	0	0	0	1	1	0	0	0
−4	0	0	0	1	1	0	0	1	0	2	0	0	0	0	0	0	0	0
2	0	0	0	0	1	1	0	0	0	0	0	1	0	0	0	0	0	1

α_f (1)	α_f+2 (5)	α_f-2 (7)	$2\alpha_f+1$ (11)	$3\alpha_f-2$ (17)	$3\alpha_f-1$ (19)	α_f+3 (23)	$2\alpha_f-3$ (23)	$\alpha_g+7(3)$	$\alpha_g+6(5)$	$\alpha_g-1(5)$	$\alpha_g(11)$	$\alpha_g+5(11)$	$\alpha_g+8(13)$	$\alpha_g-3(13)$	$\alpha_g+2(17)$	$\alpha_g+3(17)$	$-3\alpha_g+4(23)$	$3\alpha_g-5(1)$
−9		2			1			1			1			1				
−13				2						1	1						1	−1
−2			1		1				1									
−6		1		1								1						
−13												1		1				
3	2				1			1					1			1		1
						1										1		
−8		1								1			1					
	1														1			
−4								1	1									1
1											1							
3										1								
6	1							1				1						1
		1						1										1
				1					1				1					1
8	2													1				
							1		1									1
7	1		1														1	
3			2					1					1					1
3		1				1								1	1			
−4				1	1			1		2								
2					1	1						1						1

α_f (1)	α_f+2 (5)	α_f-2 (7)	$2\alpha_f+1$ (11)	$3\alpha_f-2$ (17)	$3\alpha_f-1$ (19)	α_f+3 (23)	$2\alpha_f-3$ (23)	$\alpha_g+7(3)$	$\alpha_g+6(5)$	$\alpha_g-1(5)$	$\alpha_g(11)$	$\alpha_g+5(11)$	$\alpha_g+8(13)$	$\alpha_g-3(13)$	$\alpha_g+2(17)$	$\alpha_g+3(17)$	$-3\alpha_g+4(23)$	$3\alpha_g-5(1)$
−9		2			1			−1			−1			−1				
−13				2						−1	−1						−1	1
−2			1		1				−1									
−6		1		1								−1						
−13												−1		−1				
3	2				1			−1					−1			−1		−1
						1										−1		
−8		1								−1			−1					
	1														−1			
−4								−1	−1									−1
1											−1							
3										−1								
6	1							−1				−1						−1
		1						−1										−1
				1					−1				−1					−1
8	2													−1				
							1		−1									−1
7	1		1														−1	
3			2					−1					−1					−1
3		1				1								−1	−1			
−4				1	1			−1		−2								
2					1	1						−1						−1

Example Joux–Lercier: factor basis logarithms

Right kernel $M \cdot \boldsymbol{x} = 0 \bmod (p-1)/4 = 277$:

$$\boldsymbol{x} = (\underbrace{1}_{\mathcal{U}_f}, \underbrace{21,90,83,130,102,255,51}_{\mathcal{F}_f}, \underbrace{222,183,3,1,214,79,50,21,255,111}_{\mathcal{F}_g}, \underbrace{145}_{\mathcal{U}_g})$$

Discrete Logarithms (in some basis)

Example Joux–Lercier: factor basis logarithms

Right kernel $M \cdot \boldsymbol{x} = 0 \bmod (p-1)/4 = 277$:

$$\boldsymbol{x} = (\underbrace{1}_{\mathcal{U}_f}, \underbrace{21,90,83,130,102,255,51}_{\mathcal{F}_f}, \underbrace{222,183,3,1,214,79,50,21,255,111}_{\mathcal{F}_g}, \underbrace{145}_{\mathcal{U}_g})$$

Discrete Logarithms (in some basis)

If we consider only $\mathcal{F}_g$:

- find a relation between the generator $g_0 = 2$ and $\mathcal{F}_g$
- find a relation between the target $t = 314$ and $\mathcal{F}_g$

Example Joux–Lercier: factor basis logarithms

Right kernel $M \cdot \boldsymbol{x} = 0 \bmod (p-1)/4 = 277$:

$$\boldsymbol{x} = (\underbrace{1}_{\mathcal{U}_f}, \underbrace{21,90,83,130,102,255,51}_{\mathcal{F}_f}, \underbrace{222,183,3,1,214,79,50,21,255,111}_{\mathcal{F}_g}, \underbrace{145}_{\mathcal{U}_g})$$

Discrete Logarithms (in some basis)

If we consider only $\mathcal{F}_g$:

- find a relation between the generator $g_0 = 2$ and $\mathcal{F}_g$
- find a relation between the target $t = 314$ and $\mathcal{F}_g$

But $g_0 = 2$, $t = 314$ are integers, whereas $\mathcal{F}_g$ is made of *ideals*.

Simple lift from $\mathbb{Z}/p\mathbb{Z}$ to $\mathbb{Z}[\alpha_g]$

Target $t = 314$
Wanted: $a + b\alpha_g \in \mathbb{Z}[\alpha_g]$ s.t. $\phi_g(a + b\alpha_g) = a + bm \equiv t \bmod p$
Write $t = t_0 + t_1 m$ with Euclidean division
If $|t| < |m|$, write $t + p = t_0 + t_1 m$

Simple lift from $\mathbb{Z}/p\mathbb{Z}$ to $\mathbb{Z}[\alpha_g]$

Target $t = 314$
Wanted: $a + b\alpha_g \in \mathbb{Z}[\alpha_g]$ s.t. $\phi_g(a + b\alpha_g) = a + bm \equiv t \bmod p$
Write $t = t_0 + t_1 m$ with Euclidean division
If $|t| < |m|$, write $t + p = t_0 + t_1 m$

Wanted: $a + b\alpha_g \in \mathbb{Z}[\alpha_g]$ and a, b having *small* absolute value
Write $t = t_0 + t_1 m$ with $|t_i| \approx \sqrt{m}$ with half-XGCD of (t, m)

Simple lift from $\mathbb{Z}/p\mathbb{Z}$ to $\mathbb{Z}[\alpha_g]$

Target $t = 314$
Wanted: $a + b\alpha_g \in \mathbb{Z}[\alpha_g]$ s.t. $\phi_g(a + b\alpha_g) = a + bm \equiv t \bmod p$
Write $t = t_0 + t_1 m$ with Euclidean division
If $|t| < |m|$, write $t + p = t_0 + t_1 m$

Wanted: $a + b\alpha_g \in \mathbb{Z}[\alpha_g]$ and a, b having *small* absolute value
Write $t = t_0 + t_1 m$ with $|t_i| \approx \sqrt{m}$ with half-XGCD of (t, m)

Wanted: $a + b\alpha_g \in \mathbb{Z}[\alpha_g]$ and $\mathrm{Norm}(a + b\alpha_g)$ is B_g-smooth
Write $t = t_0 + t_1 m$ with $|t_i| \approx \sqrt{m}$ with half-XGCD of (t, m)
While $\mathrm{Norm}(t_0 + t_1\alpha_g)$ is not B_g-smooth:

- $t^{(j)} \leftarrow t \cdot g^j$; $j = j + 1$
- Write $t^{(j)} = t_0 + t_1 m$ with $|t_i| \approx \sqrt{m}$ with half-XGCD of $(t^{(j)}, m)$

Simple lift from $\mathbb{Z}/p\mathbb{Z}$ to $\mathbb{Z}[\alpha_g]$

$p = 1109$, $t = 314$, $m = -347$
$t + p = 35 - 4m$ and $\text{Norm}(35 - 4\alpha_g) = 1749 = 3 \cdot 11 \cdot 53$
not B-smooth

Simple lift from $\mathbb{Z}/p\mathbb{Z}$ to $\mathbb{Z}[\alpha_g]$

$p = 1109,\ t = 314,\ m = -347$
$t + p = 35 - 4m$ and $\mathrm{Norm}(35 - 4\alpha_g) = 1749 = 3 \cdot 11 \cdot 53$
not B-smooth
$t^{(7)} = t \cdot g_0^7 = 268$
$-11 - 4m = 268 + p$, $\mathrm{Norm}(-11 - 4\alpha_g) = -275 = -5^2 \cdot 11$

Simple lift from $\mathbb{Z}/p\mathbb{Z}$ to $\mathbb{Z}[\alpha_g]$

$p = 1109,\ t = 314,\ m = -347$

$t + p = 35 - 4m$ and $\mathrm{Norm}(35 - 4\alpha_g) = 1749 = 3 \cdot 11 \cdot 53$

not B-smooth

$t^{(7)} = t \cdot g_0^7 = 268$

$-11 - 4m = 268 + p$, $\mathrm{Norm}(-11 - 4\alpha_g) = -275 = -5^2 \cdot 11$

$\gcd(-11 - 4x \bmod 5, g(x) \bmod 5) = x - 1$

$\gcd(-11 - 4x \bmod 11, g(x) \bmod 11) = x$

$$-11 - 4\alpha_g = \underbrace{(\alpha_g - 1)}_{\text{Norm } 5}{}^2 \quad \underbrace{\alpha_g}_{\text{Norm } 11} \quad / \underbrace{(3\alpha_g - 5)}_{\text{unit}}$$

Simple lift from $\mathbb{Z}/p\mathbb{Z}$ to $\mathbb{Z}[\alpha_g]$

$p = 1109,\ t = 314,\ m = -347$

$t + p = 35 - 4m$ and $\text{Norm}(35 - 4\alpha_g) = 1749 = 3 \cdot 11 \cdot 53$

not B-smooth

$t^{(7)} = t \cdot g_0^7 = 268$

$-11 - 4m = 268 + p$, $\text{Norm}(-11 - 4\alpha_g) = -275 = -5^2 \cdot 11$

$\gcd(-11 - 4x \bmod 5, g(x) \bmod 5) = x - 1$

$\gcd(-11 - 4x \bmod 11, g(x) \bmod 11) = x$

$$-11 - 4\alpha_g = \underbrace{(\alpha_g - 1)^2}_{\text{Norm } 5} \underbrace{\alpha_g}_{\text{Norm } 11} / \underbrace{(3\alpha_g - 5)}_{\text{unit}}$$

$$\begin{aligned} \log(-11 - 4\alpha_g) &= 2\log(\alpha_g - 1) + \log(\alpha_g) - \log(3\alpha_g - 5) \\ &= 2 \cdot 3 + 1 - 145 = -138 \end{aligned}$$

$\log t = -138 - 7\log g_0$

Simple lift from $\mathbb{Z}/p\mathbb{Z}$ to $\mathbb{Z}[\alpha_g]$

Same lift process with $g_0 = 2$:
$g_0^{10} = 1024 = -17 - 3m$,

Simple lift from $\mathbb{Z}/p\mathbb{Z}$ to $\mathbb{Z}[\alpha_g]$

Same lift process with $g_0 = 2$:
$g_0^{10} = 1024 = -17 - 3m$,

$$\underbrace{(-17 - 3\alpha_g)}_{\text{Norm } -65=-5\cdot 13} = -\underbrace{(\alpha_g - 1)}_{\text{Norm } 5}\underbrace{(\alpha_g - 3)}_{\text{Norm } 13} / \underbrace{(3\alpha_g - 5)}_{\text{unit}}$$

Simple lift from $\mathbb{Z}/p\mathbb{Z}$ to $\mathbb{Z}[\alpha_g]$

Same lift process with $g_0 = 2$:

$g_0^{10} = 1024 = -17 - 3m$,

$$\underbrace{(-17 - 3\alpha_g)}_{\text{Norm } -65=-5\cdot 13} = -\underbrace{(\alpha_g - 1)}_{\text{Norm } 5}\underbrace{(\alpha_g - 3)}_{\text{Norm } 13} / \underbrace{(3\alpha_g - 5)}_{\text{unit}}$$

$$\begin{aligned} \log(-17 - 3\alpha_g) &= \log(\alpha_g - 1) + \log(\alpha_g - 3) - \log(3\alpha_g - 5) \\ &= 3 + 50 - 145 = -92 \end{aligned}$$

Simple lift from $\mathbb{Z}/p\mathbb{Z}$ to $\mathbb{Z}[\alpha_g]$

Same lift process with $g_0 = 2$:

$g_0^{10} = 1024 = -17 - 3m$,

$$\underbrace{(-17 - 3\alpha_g)}_{\text{Norm } -65=-5\cdot 13} = -\underbrace{(\alpha_g - 1)}_{\text{Norm } 5}\underbrace{(\alpha_g - 3)}_{\text{Norm } 13} / \underbrace{(3\alpha_g - 5)}_{\text{unit}}$$

$$\begin{aligned} \log(-17 - 3\alpha_g) &= \log(\alpha_g - 1) + \log(\alpha_g - 3) - \log(3\alpha_g - 5) \\ &= 3 + 50 - 145 = -92 \end{aligned}$$

$\log g_0 = -92/10 \bmod 277 = 157$

Simple lift from $\mathbb{Z}/p\mathbb{Z}$ to $\mathbb{Z}[\alpha_g]$

Same lift process with $g_0 = 2$:

$g_0^{10} = 1024 = -17 - 3m$,

$$\underbrace{(-17 - 3\alpha_g)}_{\text{Norm } -65=-5\cdot 13} = -\underbrace{(\alpha_g - 1)}_{\text{Norm } 5}\underbrace{(\alpha_g - 3)}_{\text{Norm } 13} / \underbrace{(3\alpha_g - 5)}_{\text{unit}}$$

$$\begin{aligned} \log(-17 - 3\alpha_g) &= \log(\alpha_g - 1) + \log(\alpha_g - 3) - \log(3\alpha_g - 5) \\ &= 3 + 50 - 145 = -92 \end{aligned}$$

$\log g_0 = -92/10 \bmod 277 = 157$

$\log t = 148$

$\log_{g_0} t = \log t / \log g_0 = 148/157 = 8 \bmod 277$

Example Joux–Lercier: descent of the generator g_0

Reduce even more the size of the norms

Input: target t

Find

$$\phi_g\left(\frac{a+bx}{c+dx}\right)=\frac{a+bm}{c+dm}=t \bmod p$$

where $a, b, c, d \approx p^{1/4}$

Example Joux–Lercier: descent of the generator g_0

Reduce even more the size of the norms

Input: target t

Find

$$\phi_g\left(\frac{a+bx}{c+dx}\right) = \frac{a+bm}{c+dm} = t \bmod p$$

where $a, b, c, d \approx p^{1/4}$

Lattice spanned by $\{p, x-m, t, tx/x\}$

$$\begin{array}{r} \\ \\ p \rightarrow \\ x-m \rightarrow \\ t \rightarrow \\ tx/x \rightarrow \end{array} \begin{array}{c} \begin{array}{cccc} a & b & c & d \\ \downarrow & \downarrow & \downarrow & \downarrow \end{array} \\ \begin{bmatrix} p & 0 & 0 & 0 \\ -m & 1 & 0 & 0 \\ t & 0 & 1 & 0 \\ 0 & t & 0 & 1 \end{bmatrix} \end{array} \rightarrow \text{LLL} \rightarrow \begin{bmatrix} a_0 & b_0 & c_0 & d_0 \\ a_1 & b_1 & c_1 & d_1 \\ a_2 & b_2 & c_2 & d_2 \\ a_3 & b_3 & c_3 & d_3 \end{bmatrix}$$

Example Joux–Lercier: descent of the generator g_0

Reduce even more the size of the norms

Input: target t

Find

$$\phi_g\left(\frac{a+bx}{c+dx}\right) = \frac{a+bm}{c+dm} = t \bmod p$$

where $a, b, c, d \approx p^{1/4}$

Lattice spanned by $\{p, x-m, t, tx/x\}$

$$\begin{array}{r} \\ \\ p \rightarrow \\ x-m \rightarrow \\ t \rightarrow \\ tx/x \rightarrow \end{array}\begin{array}{c} \begin{array}{cccc} a & b & c & d \\ \downarrow & \downarrow & \downarrow & \downarrow \end{array} \\ \begin{bmatrix} p & 0 & 0 & 0 \\ -m & 1 & 0 & 0 \\ t & 0 & 1 & 0 \\ 0 & t & 0 & 1 \end{bmatrix} \end{array} \rightarrow \mathrm{LLL} \rightarrow \begin{bmatrix} a_0 & b_0 & c_0 & d_0 \\ a_1 & b_1 & c_1 & d_1 \\ a_2 & b_2 & c_2 & d_2 \\ a_3 & b_3 & c_3 & d_3 \end{bmatrix}$$

$$\frac{a_i + b_i m}{c_i + d_i m} = t \bmod p$$

Example Joux–Lercier: descent of the generator g_0

Try $g_0, g_0^2, g_0^3, \ldots, g_0^{12} = 769$

$$M = \begin{bmatrix} p & 0 & 0 & 0 \\ -m & 1 & 0 & 0 \\ g_0^{12} & 0 & 1 & 0 \\ 0 & g_0^{12} & 0 & 1 \end{bmatrix} \to \text{LLL} \to \begin{bmatrix} -3 & 0 & -2 & 1 \\ \mathbf{1} & \mathbf{1} & -\mathbf{3} & \mathbf{2} \\ -1 & 0 & -3 & -5 \\ -1 & 14 & 2 & -2 \end{bmatrix}$$

Example Joux–Lercier: descent of the generator g_0

Try $g_0, g_0^2, g_0^3, \ldots, g_0^{12} = 769$

$$M = \begin{bmatrix} p & 0 & 0 & 0 \\ -m & 1 & 0 & 0 \\ g_0^{12} & 0 & 1 & 0 \\ 0 & g_0^{12} & 0 & 1 \end{bmatrix} \to \text{LLL} \to \begin{bmatrix} -3 & 0 & -2 & 1 \\ \mathbf{1} & \mathbf{1} & -\mathbf{3} & \mathbf{2} \\ -1 & 0 & -3 & -5 \\ -1 & 14 & 2 & -2 \end{bmatrix}$$

$$\frac{\mathbf{1} + \mathbf{1}m}{-\mathbf{3} + \mathbf{2}m} = 769 \bmod p = g_0^{12}$$

Example Joux–Lercier: descent of the generator g_0

Try $g_0, g_0^2, g_0^3, \ldots, g_0^{12} = 769$

$$M = \begin{bmatrix} p & 0 & 0 & 0 \\ -m & 1 & 0 & 0 \\ g_0^{12} & 0 & 1 & 0 \\ 0 & g_0^{12} & 0 & 1 \end{bmatrix} \to \text{LLL} \to \begin{bmatrix} -3 & 0 & -2 & 1 \\ \mathbf{1} & \mathbf{1} & \mathbf{-3} & \mathbf{2} \\ -1 & 0 & -3 & -5 \\ -1 & 14 & 2 & -2 \end{bmatrix}$$

$$\frac{\mathbf{1} + \mathbf{1}m}{\mathbf{-3} + \mathbf{2}m} = 769 \bmod p = g_0^{12}$$

Row $(a, b) = (-1, 1)$: $-1 - \alpha_g$
Row $(a, b) = (3, -2)$: $3 - 2\alpha_g$

Example Joux–Lercier: descent of the generator g_0

Try $g_0, g_0^2, g_0^3, \ldots, g_0^{12} = 769$

$$M = \begin{bmatrix} p & 0 & 0 & 0 \\ -m & 1 & 0 & 0 \\ g_0^{12} & 0 & 1 & 0 \\ 0 & g_0^{12} & 0 & 1 \end{bmatrix} \to \text{LLL} \to \begin{bmatrix} -3 & 0 & -2 & 1 \\ \mathbf{1} & \mathbf{1} & \mathbf{-3} & \mathbf{2} \\ -1 & 0 & -3 & -5 \\ -1 & 14 & 2 & -2 \end{bmatrix}$$

$$\frac{\mathbf{1} + \mathbf{1}m}{\mathbf{-3} + \mathbf{2}m} = 769 \bmod p = g_0^{12}$$

Row $(a, b) = (-1, 1)$: $-1 - \alpha_g$
Row $(a, b) = (3, -2)$: $3 - 2\alpha_g$

$$\frac{\alpha_g + 1}{2\alpha_g - 3} = \frac{-1 - \alpha_g}{3 - 2\alpha_g} = \frac{(\alpha_g + 7)(\alpha_g + 6)(3\alpha_g - 5)}{(\alpha_g + 6)(3\alpha_g - 5)}$$

Example Joux–Lercier: descent of the generator g_0

Try $g_0, g_0^2, g_0^3, \ldots, g_0^{12} = 769$

$$M = \begin{bmatrix} p & 0 & 0 & 0 \\ -m & 1 & 0 & 0 \\ g_0^{12} & 0 & 1 & 0 \\ 0 & g_0^{12} & 0 & 1 \end{bmatrix} \to \text{LLL} \to \begin{bmatrix} -3 & 0 & -2 & 1 \\ \mathbf{1} & \mathbf{1} & \mathbf{-3} & \mathbf{2} \\ -1 & 0 & -3 & -5 \\ -1 & 14 & 2 & -2 \end{bmatrix}$$

$$\frac{\mathbf{1} + \mathbf{1}m}{\mathbf{-3} + \mathbf{2}m} = 769 \bmod p = g_0^{12}$$

Row $(a, b) = (-1, 1)$: $-1 - \alpha_g$
Row $(a, b) = (3, -2)$: $3 - 2\alpha_g$

$$\frac{\alpha_g + 1}{2\alpha_g - 3} = \frac{-1 - \alpha_g}{3 - 2\alpha_g} = \frac{(\alpha_g + 7)(\alpha_g + 6)(3\alpha_g - 5)}{(\alpha_g + 6)(3\alpha_g - 5)}$$

$$\begin{aligned} \log(g_0) &= 1/12 \log(\alpha_g + 7) = 222/12 \\ &= 157 \bmod 277 \end{aligned}$$

Example Joux–Lercier: descent of the target $t = 314$

$$M = \begin{bmatrix} 1109 & 0 & 0 & 0 \\ 347 & 1 & 0 & 0 \\ 314 & 0 & 1 & 0 \\ 0 & 314 & 0 & 1 \end{bmatrix} \to \text{LLL} \to \begin{bmatrix} \mathbf{0} & \mathbf{-1} & \mathbf{2} & \mathbf{-3} \\ 3 & 4 & 0 & 1 \\ 2 & -4 & 0 & 3 \\ -7 & 3 & 9 & 6 \end{bmatrix}$$

Example Joux–Lercier: descent of the target $t = 314$

$$M = \begin{bmatrix} 1109 & 0 & 0 & 0 \\ 347 & 1 & 0 & 0 \\ 314 & 0 & 1 & 0 \\ 0 & 314 & 0 & 1 \end{bmatrix} \to \text{LLL} \to \begin{bmatrix} \mathbf{0} & -\mathbf{1} & \mathbf{2} & -\mathbf{3} \\ 3 & 4 & 0 & 1 \\ 2 & -4 & 0 & 3 \\ -7 & 3 & 9 & 6 \end{bmatrix}$$

$$\frac{-\mathbf{1}m}{\mathbf{2} - \mathbf{3}m} = 314 \bmod p$$

Example Joux–Lercier: descent of the target $t = 314$

$$M = \begin{bmatrix} 1109 & 0 & 0 & 0 \\ 347 & 1 & 0 & 0 \\ 314 & 0 & 1 & 0 \\ 0 & 314 & 0 & 1 \end{bmatrix} \to \text{LLL} \to \begin{bmatrix} \mathbf{0} & \mathbf{-1} & \mathbf{2} & \mathbf{-3} \\ 3 & 4 & 0 & 1 \\ 2 & -4 & 0 & 3 \\ -7 & 3 & 9 & 6 \end{bmatrix}$$

$$\frac{\mathbf{-1}m}{\mathbf{2} - \mathbf{3}m} = 314 \bmod p$$

Row $(a, b) = (0, 1)$: $-\alpha_g$
Row $(a, b) = (2, 3)$: $2 - 3\alpha_g$

Example Joux–Lercier: descent of the target $t = 314$

$$M = \begin{bmatrix} 1109 & 0 & 0 & 0 \\ 347 & 1 & 0 & 0 \\ 314 & 0 & 1 & 0 \\ 0 & 314 & 0 & 1 \end{bmatrix} \to \text{LLL} \to \begin{bmatrix} \mathbf{0} & -\mathbf{1} & \mathbf{2} & -\mathbf{3} \\ 3 & 4 & 0 & 1 \\ 2 & -4 & 0 & 3 \\ -7 & 3 & 9 & 6 \end{bmatrix}$$

$$\frac{-\mathbf{1}m}{\mathbf{2} - \mathbf{3}m} = 314 \bmod p$$

Row $(a, b) = (0, 1)$: $-\alpha_g$
Row $(a, b) = (2, 3)$: $2 - 3\alpha_g$

$$\frac{-\alpha_g}{2 - 3\alpha_g} = \frac{-\alpha_g}{(\alpha_g + 6)(\alpha_g + 8)(-3\alpha_g + 5)}$$

Example Joux–Lercier: descent of the target $t = 314$

$$M = \begin{bmatrix} 1109 & 0 & 0 & 0 \\ 347 & 1 & 0 & 0 \\ 314 & 0 & 1 & 0 \\ 0 & 314 & 0 & 1 \end{bmatrix} \rightarrow \text{LLL} \rightarrow \begin{bmatrix} \mathbf{0} & -\mathbf{1} & \mathbf{2} & -\mathbf{3} \\ 3 & 4 & 0 & 1 \\ 2 & -4 & 0 & 3 \\ -7 & 3 & 9 & 6 \end{bmatrix}$$

$$\frac{-\mathbf{1}m}{\mathbf{2} - \mathbf{3}m} = 314 \bmod p$$

Row $(a, b) = (0, 1)$: $-\alpha_g$
Row $(a, b) = (2, 3)$: $2 - 3\alpha_g$

$$\frac{-\alpha_g}{2 - 3\alpha_g} = \frac{-\alpha_g}{(\alpha_g + 6)(\alpha_g + 8)(-3\alpha_g + 5)}$$

$$\begin{aligned} \log(t) &= \log(\alpha_g) - \log(\alpha_g + 6) - \log(\alpha_g + 8) - \log(-3\alpha_g + 5) \\ &= 1 - 183 - 79 - 145 \\ &= 148 \bmod 277 \end{aligned}$$

Example Joux–Lercier

Finally,
$\log_{g_0} t = \log t / \log g_0 = 148/157 = 8 \bmod 277$
$314/g_0^8 = g_0^{3(p-1)/4}$
$\log_{g_0} t = 8 + 3(p-1)/4 = 839 \bmod 1108$

$g_0^{839} = 314 \bmod p$
$\log_{g_0} 314 = 839$

As expected.

Generalized descent with Joux–Lercier

Given $t \in \mathbb{Z}/p\mathbb{Z}$, and $f(x)$ of degree $d+1$, find

$$\frac{\boldsymbol{a}(x)}{\boldsymbol{b}(x)} = \frac{a_0 + a_1 x + \ldots + a_d x^d}{b_0 + b_1 x + \ldots + b_d x^d} \ s.t.\ \frac{\boldsymbol{a}(m)}{\boldsymbol{b}(m)} = t \bmod p$$

Generalized descent with Joux–Lercier

Given $t \in \mathbb{Z}/p\mathbb{Z}$, and $f(x)$ of degree $d+1$, find

$$\frac{\boldsymbol{a}(x)}{\boldsymbol{b}(x)} = \frac{a_0 + a_1 x + \ldots + a_d x^d}{b_0 + b_1 x + \ldots + b_d x^d} \; s.t. \; \frac{\boldsymbol{a}(m)}{\boldsymbol{b}(m)} = t \bmod p$$

$$\begin{array}{r} \\ \\ p \rightarrow \\ x-m \rightarrow \\ x^i(x-m) \rightarrow \\ x^d(x-m) \rightarrow \\ t \rightarrow \\ tx/x \rightarrow \\ tx^i/x^i \rightarrow \\ tx^d/x^d \rightarrow \end{array}
\begin{array}{c} \begin{array}{cccccccc} a_0 & & & a_d & b_0 & & & b_d \\ \downarrow & & & \downarrow & \downarrow & & & \downarrow \end{array} \\
\left[\begin{array}{cccc|cccc} p & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ -m & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ & \ddots & \ddots & & & & & \\ 0 & 0 & -m & 1 & 0 & 0 & 0 & 0 \\ \hline t & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & t & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & \ddots & 0 & 0 & 0 & \ddots & 0 \\ 0 & 0 & 0 & t & 0 & 0 & 0 & 1 \end{array}\right] \end{array}
\rightarrow \text{LLL} \rightarrow
\left[\begin{array}{c} a_0 \ldots a_d \;\; b_0 \ldots b_d \\ \\ \\ * \\ \\ \\ \end{array}\right]$$

Generalized descent with Joux–Lercier

$f = x^3 - x + 1,\ g = 2,\ t = 314$

$$M = \begin{bmatrix} p & 0 & 0 & 0 & 0 & 0 \\ -m & 1 & 0 & 0 & 0 & 0 \\ 0 & -m & 1 & 0 & 0 & 0 \\ t & 0 & 0 & 1 & 0 & 0 \\ 0 & t & 0 & 0 & 1 & 0 \\ 0 & 0 & t & 0 & 0 & 1 \end{bmatrix} \rightarrow \text{LLL} \rightarrow \begin{bmatrix} -1 & 0 & 0 & -1 & 0 & -2 \\ -1 & 0 & 1 & -1 & -2 & 1 \\ 0 & -1 & 0 & 2 & -3 & 0 \\ 3 & -1 & 1 & 0 & -1 & -1 \\ -2 & -1 & 3 & 1 & 1 & 0 \\ \mathbf{-2} & \mathbf{-4} & \mathbf{-1} & \mathbf{1} & \mathbf{1} & \mathbf{-1} \end{bmatrix}$$

$$\frac{-2 - 4m - m^2}{1 + m - m^2} = 314 \bmod p$$

$$\frac{\text{Norm}(-2 - 4\alpha_f - \alpha_f^2)}{\text{Norm}(1 + \alpha_f - \alpha_f^2)} = \frac{7^2}{-5} \rightarrow \frac{-2 - 4\alpha_f - \alpha_f^2}{1 + \alpha_f - \alpha_f^2} = \frac{-(\alpha_f - 2)^2 \alpha_f^{-7}}{-(\alpha_f + 2)\alpha_f^4}$$

$\log t = 2 \cdot 90 - 7 - 21 - 4 = 148$

With similar technique, one obtains $\log g = 157$

Finally $\log_g t = 148/157 = 8$

DL record computation in 2017: 768-bit $\mathbb{F}_p$

Kleinjung, Diem, A. Lenstra, Priplata, Stahlke, Eurocrypt'2017.
$p = \lfloor 2^{766} \times \pi \rfloor + 62762$ prime, 768 bits, 232 decimal digits, $p =$

12193448583342869326963419091957961095266573861542513280 29
27365617576687098030650558457738912586082671520154722579 40
72935883258868036433287217994721542199148182841505800433 14
84108696835906593468476595191083938374145678927305791623 19

$(p-1)/2$ prime

$f(x) = 140x^4 + 34x^3 + 86x^2 + 5x - 55$

$$\begin{aligned} g(x) = {} & 370863403886416141150505523919527677231932618184100095924x^3 \\ & -1937981312833038778565617469829395544065255938015920309679x^2 \\ & -217583293626947899787577441128333027617541095004734736415x \\ & +277260730400349522890422618473498148528706115003337935150 \end{aligned}$$

Enumerate ($\sim 10^{12}$) all $f(x)$ s.t. $|f_i| \leqslant 165$
By construction, $|g_i| \approx p^{1/4}$

DL record computation in 2017: 768-bit $\mathbb{F}_p$

$\gcd(f, g) = 1$ in $\mathbb{Q}[x]$
$\exists$ root m s.t. $f(m) = g(m) = 0 \pmod p$, $m =$

42902956292319703574889360640139954233871229273731672191128794979019508571426956110520280493413148710512618823586632148449741318839265324620677402775664644418324062965090411211026991626107428130330288372525887846431331219647577522

Multiplicative relations: for all $|a|, |b| \leq A \approx 2^{32}$, $\gcd(a, b) = 1$

- factor Resultant$(f, a + bx) \approx 130$ bits, 39 dd
- factor Resultant$(g, a + bx) \approx 290$ bits, 87 dd

Linear algebra: square sparse matrix of $23.5 \cdot 10^6$ rows
Total time: 5300 core-years on Intel Xeon E5-2660 2.2GHz

NFS: internal algorithms

- NFS: Gordon 93, improvements Schirokauer 93
- polynomial selection Joux–Lercier 03
- Franke–Kleinjung 08 sieve, ECM factorization H. Lenstra 87
- Schirokauer 93 maps (to deal with units)
- block Lanczos, Wiedemann 86 sparse linear algebra
- Joux–Lercier 03 descent, early-abort strategy Pomerance 82

NFS for factoring

See Jeremie Detrey's talk at Arith'22 follow-up
`http://www.ens-lyon.fr/LIP/AriC/tutorials-june-25-2015`

L. Adleman.
A subexponential algorithm for the discrete logarithm problem with applications to cryptography.
In *20th FOCS*, pages 55–60. IEEE Computer Society Press, oct 1979.
https://doi.org/10.1109/SFCS.1979.2.

E. R. Canfield, P. Erdős, and C. Pomerance.
On a problem of Oppenheim concerning “factorisatio numerorum”.
Journal of Number Theory, 17(1):1–28, 1983.
https://doi.org/10.1016/0022-314X(83)90002-1,
https://math.dartmouth.edu/~carlp/PDF/paper39.pdf.

D. Coppersmith.
Fast evaluation of logarithms in fields of characteristic two.
IEEE Transactions on Information Theory, 30(4):587–594, 1984.
http://ieeexplore.ieee.org/document/1056941/,
https://doi.org/10.1109/TIT.1984.1056941.

D. Coppersmith, A. M. Odlyzko, and R. Schroeppel.
Discrete logarithms in GF(p).
Algorithmica, 1(1):1–15, 1986.
https://dl.acm.org/citation.cfm?id=6835,
https://doi.org/10.1007/BF01840433.

W. Eberly and E. Kaltofen.
On randomized Lanczos algorithm.
In W. W. Küchlin, editor, *Proceedings of the 1997 International Symposium on Symbolic and Algebraic Computation*, ISSAC '97, pages 176–183, New York, NY, USA, July 21–23 1997. ACM.
http://doi.acm.org/10.1145/258726.258776.

D. M. Gordon.
Discrete logarithms in GF(p) using the number field sieve.
SIAM Journal on Discrete Mathematics, 6(1):124–138, 1993.
https://www.ccrwest.org/gordon/log.pdf.

A. Joux and R. Lercier.
Improvements to the general number field sieve for discrete logarithms in prime fields. A comparison with the Gaussian integer method.
Math. Comp., 72(242):953–967, 2003.
https://doi.org/10.1090/S0025-5718-02-01482-5,
http://www.ams.org/journals/mcom/2003-72-242/S0025-5718-02-01482-5.

A. Joux, R. Lercier, N. Smart, and F. Vercauteren.
The number field sieve in the medium prime case.
In C. Dwork, editor, *CRYPTO 2006*, volume 4117 of *LNCS*, pages 326–344. Springer, Heidelberg, Aug. 2006.
https://www.iacr.org/archive/crypto2006/41170323/41170323.pdf.

T. Kleinjung, C. Diem, A. K. Lenstra, C. Priplata, and C. Stahlke.
Computation of a 768-bit prime field discrete logarithm.
In J. Coron and J. B. Nielsen, editors, *EUROCRYPT 2017, Part I*, volume 10210 of *LNCS*, pages 185–201. Springer, Heidelberg, Apr. / May 2017.
https://eprint.iacr.org/2017/067.

M. Kraitchik.
Théorie des Nombres.
Gauthier–Villars, 1922.

M. Kraitchik.
Recherches sur la Théorie des Nombres.
Gauthier–Villars, 1924.

H. Lenstra and C. Pomerance.
A rigorous time bound for factoring integers.
J. Amer. Math. Soc., 5(3):483–516, 1992.
https://doi.org/10.1090/S0894-0347-1992-1137100-0.

H. W. Lenstra.
Factoring integers with elliptic curves.
Annals of Mathematics, 126(3):649–673, 1987.
https://doi.org/10.2307/1971363,http://www.jstor.org/stable/1971363.

K. S. McCurley.
The discrete logarithm problem.
In C. Pomerance, editor, *Cryptology and Computational Number Theory*, volume 42 of *Proceedings of Symposia in Applied Mathematics*, pages 49–74. AMS, 1990.
https://bookstore.ams.org/psapm-42/,
http://www.mccurley.org/papers/dlog.pdf.

C. Pomerance.
Analysis and comparison of some integer factoring algorithms.
In H. W. J. Lenstra and R. Tijdeman, editors, *Computational methods in number theory, part I*, volume 154 of *Mathematical Centre Tracts*, pages 89–139. Mathematisch Centrum, Amsterdam, 1982.
http://oai.cwi.nl/oai/asset/19571/19571A.pdf.

C. Pomerance.
Fast, rigorous factorization and discrete logarithm algorithms.
In D. S. Johnson, T. Nishizeki, A. Nozaki, and H. S. Wilf, editors, *Discrete Algorithms and Complexity*, pages 119–143. Academic Press, Orlando, Florida, 1987.
https://doi.org/10.1016/B978-0-12-386870-1.50014-9,
https://math.dartmouth.edu/~carlp/disclog.pdf.

O. Schirokauer.
Discrete logarithms and local units.
Philos. Trans. Roy. Soc. London Ser. A, 345(1676):409–423, 1993.
http://rsta.royalsocietypublishing.org/content/345/1676/409,
http://doi.org/10.1098/rsta.1993.0139.

I. N. Stewart and D. O. Tall.
Algebraic Number Theory and Fermat's Last Theorem.
Chapman and Hall/CRC, 4th edition, October 2015.
Textbook - 322 Pages - 21 B/W Illustrations.

D. Weber.
An implementation of the general number field sieve to compute discrete logarithms mod p.
In L. C. Guillou and J.-J. Quisquater, editors, *EUROCRYPT'95*, volume 921 of *LNCS*, pages 95–105. Springer, Heidelberg, May 1995.

D. Weber.
Computing discrete logarithms with quadratic number rings.
In K. Nyberg, editor, *EUROCRYPT'98*, volume 1403 of *LNCS*, pages 171–183. Springer, Heidelberg, May / June 1998.
https://doi.org/10.1007/BFb0054125.

D. Weber and T. F. Denny.
The solution of McCurley's discrete log challenge.
In H. Krawczyk, editor, *CRYPTO'98*, volume 1462 of *LNCS*, pages 458–471. Springer, Heidelberg, Aug. 1998.
https://doi.org/10.1007/BFb0055747.

A. E. Western and J. C. P. Miller.
Tables of Indices and Primitive Roots, volume 9 of *Royal Society Mathematical Tables*.
Cambridge University Press, 1968.

D. H. Wiedemann.
Solving sparse linear equations over finite fields.
IEEE Trans. Inform. Theory, IT–32(1):54–62, Jan 1986.
https://doi.org/10.1109/TIT.1986.1057137.