Logarithms

James McKee

June 26, 2013

Plan

- Logarithmic functions and logarithms

Plan

- Logarithmic functions and logarithms
- Standard examples

Plan

- Logarithmic functions and logarithms
- Standard examples
- History and motivation

Plan

- Logarithmic functions and logarithms

- Standard examples

- History and motivation

- k-radius primes

Plan

- Logarithmic functions and logarithms
- Standard examples
- History and motivation
- k-radius primes
- Computational and theoretical results

Plan

- Logarithmic functions and logarithms
- Standard examples
- History and motivation
- k-radius primes
- Computational and theoretical results
- Open problem

Logarithmic functions

A **logarithmic function** (of length k) is a function

$$f : \{1, 2, \ldots, k\} \to \mathbb{Z}/k\mathbb{Z}$$

satisfying

$$f(ab) = f(a) + f(b)$$

whenever both sides make sense (i.e., whenever a, b, $ab \in \{1, 2, \ldots, k\}$).

Logarithmic functions

A **logarithmic function** (of length k) is a function

$$f : \{1, 2, \ldots, k\} \to \mathbb{Z}/k\mathbb{Z}$$

satisfying

$$f(ab) = f(a) + f(b)$$

whenever both sides make sense (i.e., whenever a, b, $ab \in \{1, 2, \ldots, k\}$).

Logarithmic functions

A **logarithmic function** (of length k) is a function

$$f : \{1, 2, \ldots, k\} \to \mathbb{Z}/k\mathbb{Z}$$

satisfying

$$f(ab) = f(a) + f(b)$$

whenever both sides make sense (i.e., whenever a, b, $ab \in \{1, 2, \ldots, k\}$).

There are $k^{\pi(k)}$ logarithmic functions of length k: the primes below k can be assigned arbitrary images, and then all other values are determined by the logarithmic property.

Logarithmic functions

A **logarithmic function** (of length k) is a function

$$f : \{1, 2, \ldots, k\} \to \mathbb{Z}/k\mathbb{Z}$$

satisfying

$$f(ab) = f(a) + f(b)$$

whenever both sides make sense (i.e., whenever a, b, $ab \in \{1, 2, \ldots, k\}$).

We must have $f(1) = 0$.

Logarithmic functions

A **logarithmic function** (of length k) is a function

$$f : \{1, 2, \ldots, k\} \to \mathbb{Z}/k\mathbb{Z}$$

satisfying

$$f(ab) = f(a) + f(b)$$

whenever both sides make sense (i.e., whenever a, b, $ab \in \{1, 2, \ldots, k\}$).

Some examples arise naturally . . .

Logarithmic functions: example

Suppose that $p = k + 1$ is prime, and that g generates $(\mathbb{Z}/p\mathbb{Z})^*$.

Given $a \in \{1, \ldots, k\}$, we can view a as an element of $(\mathbb{Z}/p\mathbb{Z})^*$, and define $f(a)$ by

$$a = g^{f(a)},$$

the discrete logarithm of a to base g.

Then f is a logarithmic function.

Logarithmic functions: example

Suppose that $p = k + 1$ is prime, and that g generates $(\mathbb{Z}/p\mathbb{Z})^*$.

Given $a \in \{1, \ldots, k\}$, we can view a as an element of $(\mathbb{Z}/p\mathbb{Z})^*$, and define $f(a)$ by

$$a = g^{f(a)},$$

the discrete logarithm of a to base g.

Then f is a logarithmic function.

N.B., the definition of a logarithmic function does not here require $f(c) = f(a) + f(b)$ whenever $c \equiv ab \pmod{p}$, although this is true.

Logarithmic functions: example

Suppose that $p = k + 1$ is prime, and that g generates $(\mathbb{Z}/p\mathbb{Z})^*$.

Given $a \in \{1, \ldots, k\}$, we can view a as an element of $(\mathbb{Z}/p\mathbb{Z})^*$, and define $f(a)$ by

$$a = g^{f(a)} ,$$

the discrete logarithm of a to base g.

Then f is a logarithmic function.

In the example above, f is bijective. This is not a requirement for logarithmic functions in general, and when it happens we endow our logarithmic function with a special name ...

Logarithms

- A **logarithm** of length k is a bijective logarithmic function of length k.

Logarithms

- A **logarithm** of length k is a bijective logarithmic function of length k.

- We have seen that if $k + 1$ is prime, then there exists a logarithm of length k.

Logarithms

- A **logarithm** of length k is a bijective logarithmic function of length k.

- We have seen that if $k+1$ is prime, then there exists a logarithm of length k. (Indeed there are at least $\varphi(k)$ logarithms, coming from the different choices for generators of $(\mathbb{Z}/(k+1)\mathbb{Z})^*$.)

Logarithms

- A **logarithm** of length k is a bijective logarithmic function of length k.

- We have seen that if $k+1$ is prime, then there exists a logarithm of length k. (Indeed there are at least $\varphi(k)$ logarithms, coming from the different choices for generators of $(\mathbb{Z}/(k+1)\mathbb{Z})^*$.)

- There are other examples...

Logarithms: another family of examples

Suppose that $p = 2k + 1$ is prime.

Let $\widehat{f}(a) \in \mathbb{Z}/2k\mathbb{Z}$ be a discrete logarithm in $(\mathbb{Z}/p\mathbb{Z})^*$.

Logarithms: another family of examples

Suppose that $p = 2k + 1$ is prime.

Let $\widehat{f}(a) \in \mathbb{Z}/2k\mathbb{Z}$ be a discrete logarithm in $(\mathbb{Z}/p\mathbb{Z})^*$.

Let $\pi : \mathbb{Z}/2k\mathbb{Z} \to \mathbb{Z}/k\mathbb{Z}$ be the natural surjection.

Logarithms: another family of examples

Suppose that $p = 2k + 1$ is prime.

Let $\widehat{f}(a) \in \mathbb{Z}/2k\mathbb{Z}$ be a discrete logarithm in $(\mathbb{Z}/p\mathbb{Z})^*$.

Let $\pi : \mathbb{Z}/2k\mathbb{Z} \to \mathbb{Z}/k\mathbb{Z}$ be the natural surjection.

Define $f : \{1, \ldots, k\} \to \mathbb{Z}/k\mathbb{Z}$ by $f(a) = \pi(\widehat{f}(a))$.

Logarithms: another family of examples

Suppose that $p = 2k + 1$ is prime.

Let $\widehat{f}(a) \in \mathbb{Z}/2k\mathbb{Z}$ be a discrete logarithm in $(\mathbb{Z}/p\mathbb{Z})^*$.

Let $\pi : \mathbb{Z}/2k\mathbb{Z} \to \mathbb{Z}/k\mathbb{Z}$ be the natural surjection.

Define $f : \{1, \ldots, k\} \to \mathbb{Z}/k\mathbb{Z}$ by $f(a) = \pi(\widehat{f}(a))$.

This is certainly a logarithmic function of length k.

Logarithms: another family of examples

Suppose that $p = 2k + 1$ is prime.

Let $\widehat{f}(a) \in \mathbb{Z}/2k\mathbb{Z}$ be a discrete logarithm in $(\mathbb{Z}/p\mathbb{Z})^*$.

Let $\pi : \mathbb{Z}/2k\mathbb{Z} \to \mathbb{Z}/k\mathbb{Z}$ be the natural surjection.

Define $f : \{1, \ldots, k\} \to \mathbb{Z}/k\mathbb{Z}$ by $f(a) = \pi(\widehat{f}(a))$.

This is certainly a logarithmic function of length k.

If $f(a) = f(b)$, then either $a = b$ or $a \equiv -b \pmod{p}$;

Logarithms: another family of examples

Suppose that $p = 2k + 1$ is prime.

Let $\widehat{f}(a) \in \mathbb{Z}/2k\mathbb{Z}$ be a discrete logarithm in $(\mathbb{Z}/p\mathbb{Z})^*$.

Let $\pi : \mathbb{Z}/2k\mathbb{Z} \to \mathbb{Z}/k\mathbb{Z}$ be the natural surjection.

Define $f : \{1, \ldots, k\} \to \mathbb{Z}/k\mathbb{Z}$ by $f(a) = \pi(\widehat{f}(a))$.

This is certainly a logarithmic function of length k.

If $f(a) = f(b)$, then either $a = b$ or $a \equiv -b \pmod{p}$; for a and b between 1 and k, the latter is not possible, so f is injective, and hence bijective.

Logarithms: the story so far

- There are logarithms of length k whenever either $k+1$ is prime or $2k+1$ is prime.

Logarithms: the story so far

- There are logarithms of length k whenever either $k+1$ is prime or $2k+1$ is prime.

- There are examples of logarithms that do not arise from discrete logarithms as above.

Logarithms: the story so far

- There are logarithms of length k whenever either $k+1$ is prime or $2k+1$ is prime.

- There are examples of logarithms that do not arise from discrete logarithms as above.

- Some of these other examples have number-theoretic manifestations, coming from k-th power residue symbols.

Logarithms: the story so far

- There are logarithms of length k whenever either $k+1$ is prime or $2k+1$ is prime.

- There are examples of logarithms that do not arise from discrete logarithms as above.

- Some of these other examples have number-theoretic manifestations, coming from k-th power residue symbols. (Some do not, although every example of odd length arises in this way.)

Logarithms: the story so far

- There are logarithms of length k whenever either $k + 1$ is prime or $2k + 1$ is prime.

- There are examples of logarithms that do not arise from discrete logarithms as above.

- Some of these other examples have number-theoretic manifestations, coming from k-th power residue symbols. (Some do not, although every example of odd length arises in this way.)

- As soon as a logarithm of length k exists, one can scale it to get $\varphi(k)$ others.

Logarithms: the story so far

- There are examples of logarithms that do not arise from discrete logarithms as above.

- Some of these other examples have number-theoretic manifestations, coming from k-th power residue symbols. (Some do not, although every example of odd length arises in this way.)

- As soon as a logarithm of length k exists, one can scale it to get $\varphi(k)$ others.

- One can also shuffle the values of the logarithms of certain primes.

Logarithms: the story so far

- Some of these other examples have number-theoretic manifestations, coming from k-th power residue symbols. (Some do not, although every example of odd length arises in this way.)

- As soon as a logarithm of length k exists, one can scale it to get $\varphi(k)$ others.

- One can also shuffle the values of the logarithms of certain primes.

- Logarithms of length k exist for all $k < 195$ (more on larger k later).

Logarithms: the story so far

- As soon as a logarithm of length k exists, one can scale it to get $\varphi(k)$ others.

- One can also shuffle the values of the logarithms of certain primes.

- Logarithms of length k exist for all $k < 195$ (more on larger k later).

- $k = 184$ is the smallest length for which a logarithm exists, but for which there is no logarithm of that length coming from any of the above number-theoretic ideas.

Logarithms: motivation

Logarithms have appeared in a number of settings:

- construction of lattice tilings;

Logarithms: motivation

Logarithms have appeared in a number of settings:

- construction of lattice tilings;
- group theory

Logarithms: motivation

Logarithms have appeared in a number of settings:

- construction of lattice tilings;
- group theory
- number theory

Logarithms: motivation

Logarithms have appeared in a number of settings:

- construction of lattice tilings;
- group theory
- number theory
- coding theory

A digression: k-radius sequences

An n-ary k-radius sequence is a finite sequence from the alphabet $\{0, 1, \ldots, n-1\}$ such that any 2 distinct elements of the alphabet are at most k terms apart in the sequence.

A digression: k-radius sequences

An n-ary k-radius sequence is a finite sequence from the alphabet $\{0, 1, \ldots, n-1\}$ such that any 2 distinct elements of the alphabet are at most k terms apart in the sequence.

In other words, if one slides a window that covers $k+1$ terms of the sequence along the sequence, then every possible pair of elements is seen through the window at some point.

A digression: k-radius sequences

An n-ary k-radius sequence is a finite sequence from the alphabet $\{0, 1, \ldots, n-1\}$ such that any 2 distinct elements of the alphabet are at most k terms apart in the sequence.

In other words, if one slides a window that covers $k+1$ terms of the sequence along the sequence, then every possible pair of elements is seen through the window at some point.

These have been used in certain caching strategies.

A digression: k-radius sequences

For example, here is a 5-ary 2-radius sequence:

0	1	2	3	4	0	1

A digression: k-radius sequences

For example, here is a 5-ary 2-radius sequence:

0	1	2	3	4	0	1

A digression: k-radius sequences

For example, here is a 5-ary 2-radius sequence:

0	1	2	3	4	0	1

A digression: k-radius sequences

For example, here is a 5-ary 2-radius sequence:

0	1	2	3	4	0	1

A digression: k-radius sequences

For example, here is a 5-ary 2-radius sequence:

0	1	2	3	4	0	1

A digression: k-radius sequences

For example, here is a 5-ary 2-radius sequence:

0	1	2	3	4	0	1

A digression: k-radius primes

A k-radius prime is a prime p such that:

- $p \equiv 1 \pmod{2k}$;
- the elements $1^{(p-1)/k}$, $2^{(p-1)/k}$, $\ldots$, $k^{(p-1)/k}$ are pairwise distinct when reduced modulo p.

A digression: k-radius primes

A k-radius prime is a prime p such that:

- $p \equiv 1 \pmod{2k}$;
- the elements $1^{(p-1)/k}$, $2^{(p-1)/k}$, $\ldots$, $k^{(p-1)/k}$ are pairwise distinct when reduced modulo p.

Note that the listed elements are kth roots of unity modulo p, and there are only k of these.

A digression: k-radius primes

A k-radius prime is a prime p such that:

- $p \equiv 1 \pmod{2k}$;
- the elements $1^{(p-1)/k}$, $2^{(p-1)/k}$, $\ldots$, $k^{(p-1)/k}$ are pairwise distinct when reduced modulo p.

Taking discrete logs with any chosen k-th root of unity as a base gives a logarithm of length k.

A digression: k-radius primes and sequences

Proposition (Blackburn,M [2012])

If p is a k-radius prime, then there is a p-ary k-radius sequence of length

$$(p+k-1)(p-1)/(2k)+1\,.$$

A digression: k-radius primes and sequences

Proposition (Blackburn,M [2012])

If p is a k-radius prime, then there is a p-ary k-radius sequence of length

$$(p + k - 1)(p - 1)/(2k) + 1\,.$$

This is asymptotically good: it is easy to see that the length has to be greater than $p(p - 1)/(2k)$.

A digression: k-radius primes and sequences

Proposition (Blackburn,M [2012])

If p is a k-radius prime, then there is a p-ary k-radius sequence of length

$$(p+k-1)(p-1)/(2k)+1\,.$$

We also constructed k-radius sequences from logarithms, going via tilings.

A digression: k-radius primes and logarithms

Let $k = 7$.

A digression: k-radius primes and logarithms

Let $k = 7$. (Note that neither $k + 1$ nor $2k + 1$ is a prime.)

A digression: k-radius primes and logarithms

Let k = 7. (Note that neither $k + 1$ nor $2k + 1$ is a prime.)

Let $p = 659$ (the smallest prime for which this trick works).

A digression: k-radius primes and logarithms

Let $k = 7$. (Note that neither $k + 1$ nor $2k + 1$ is a prime.)

Let $p = 659$ (the smallest prime for which this trick works).

$1^{94}, 2^{94}, \ldots, 7^{94}$ happen to be distinct mod 659.

A digression: k-radius primes and logarithms

Let k = 7. (Note that neither $k + 1$ nor $2k + 1$ is a prime.)

Let $p = 659$ (the smallest prime for which this trick works).

1^{94}, 2^{94}, . . . , 7^{94} happen to be distinct mod 659.

Writing them to base 307, they are 307^0, 307^1, 307^4, 307^2, 307^3, 307^5, 307^6. Hence . . .

A digression: k-radius primes and logarithms

$$\begin{array}{ccc} 1 & & 0 \\ 2 & & 1 \\ 3 & & 4 \\ 4 & \mapsto & 2 \\ 5 & & 3 \\ 6 & & 5 \\ 7 & & 6 \end{array}$$

is a logarithm of length 7.

Logarithms from number theory

Taking any prime $\equiv 1 \pmod{k}$, we can always get a logarithmic function in this way, but getting a logarithm is much more rare.

Logarithms from number theory

Taking any prime $\equiv 1 \pmod{k}$, we can always get a logarithmic function in this way, but getting a logarithm is much more rare.

Working in cyclotomic fields, and using density results for primes with certain character values, one can show:

Theorem (Mills, 1963) If k is odd, then any logarithmic function (and hence any logarithm) arises in this way. Indeed for infinitely many primes.

Logarithms from number theory

Taking any prime $\equiv 1 \pmod{k}$, we can always get a logarithmic function in this way, but getting a logarithm is much more rare.

Working in cyclotomic fields, and using density results for primes with certain character values, one can show:

Theorem (Mills, 1963) If k is odd, then any logarithmic function (and hence any logarithm) arises in this way. Indeed for infinitely many primes.

Elliott (1970) gave the density, with an estimate for the error.

Logarithms from number theory: k even

Consider $k = 10$. (Yes, we know already that a logarithm exists!)

Logarithms from number theory: k even

Consider $k = 10$. (Yes, we know already that a logarithm exists!)

For any $p \equiv 1 \pmod{k}$, we have

$$\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = \left(\frac{1}{5}\right) = 1\,.$$

Logarithms from number theory: k even

Consider $k = 10$. (Yes, we know already that a logarithm exists!)

For any $p \equiv 1 \pmod{k}$, we have

$$\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = \left(\frac{1}{5}\right) = 1\,.$$

So 5 is a square mod p, and $5^{(p-1)/10}$ is a square of a 10th root of unity, so cannot be a primitive 10th root of unity.

Logarithms from number theory: k even

So

$$\begin{array}{cccccccccc} 1 & 2 & 3 & 4 & \color{blue}{5} & 6 & 7 & 8 & 9 & 10 \\ & & & & & \downarrow & & & & \\ 0 & 4 & 3 & 8 & \color{blue}{1} & 7 & 9 & 2 & 6 & 5 \end{array}$$

is an example of a logarithm that does not come from computing discrete logarithms in the 10th roots of unity modulo *any* prime.

Logarithms from number theory: k even

Mills (1963) showed that when k is even a logarithmic function f comes from discrete logarithms in the kth roots of unity modulo p for some prime p (and indeed infinitely many) if and only if

$f(m)$ is even if one of the following holds:

- $m \mid k$ and $m \equiv 1 \pmod 4$;
- $4m \mid k$.

Logarithms from number theory: k even

For k-radius primes, the condition is slightly simpler.

A logarithm f of length k comes from a k-radius prime if and only if

$$\boxed{\bullet \text{ if } 2m \mid k \text{ then } f(m) \text{ is even.}}$$

Logarithms from number theory: k even

For k-radius primes, the condition is slightly simpler.

A logarithm f of length k comes from a k-radius prime if and only if

$$\boxed{\bullet \text{ if } 2m \mid k \text{ then } f(m) \text{ is even.}}$$

This works for odd and even k!

Logarithms from number theory: k even

For k-radius primes, the condition is slightly simpler.

A logarithm f of length k comes from a k-radius prime if and only if

$$\boxed{\bullet \text{ if } 2m \mid k \text{ then } f(m) \text{ is even.}}$$

One can show that this condition implies Mills' condition in all cases.

Logarithms: some terminology

Those logarithms that come from primes $\equiv 1 \pmod{k}$ we call **KM-logarithms** (Kummer-Mills).

Logarithms: some terminology

Those logarithms that come from primes $\equiv 1 \pmod{k}$ we call **KM-logarithms** (Kummer-Mills).

Those that come from k-radius primes are more special: we call them **special KM-logarithms**.

Logarithms: computational results

For $k \leq 300$, there are logarithms of length k **except** for

$$k = 195, 205, 208, 211, 212, 214, 217, 218, 220, 227, 229, 235, 242, 244, 246\text{–}248, 252, 253, 255, 257\text{–}259, 263\text{–}267, 269, 271, 274, 275, 279, 283, 286, 287, 289\text{–}291, 294, 295, 297, 298.$$

Logarithms: computational results

For $k \leq 300$, there are logarithms of length k **except** for

$$k = 195, 205, 208, 211, 212, 214, 217, 218, 220, 227, 229, 235, 242, 244, 246\text{–}248, 252, 253, 255, 257\text{–}259, 263\text{–}267, 269, 271, 274, 275, 279, 283, 286, 287, 289\text{–}291, 294, 295, 297, 298.$$

In addition, there are no KM-logarithms of length k for

$$k = 184, 234, 236.$$

Logarithms: computational results

For $k \leq 300$, there are logarithms of length k **except** for

$$k = 195, 205, 208, 211, 212, 214, 217, 218, 220, 227, 229, 235, 242, 244, 246\text{–}248, 252, 253, 255, 257\text{–}259, 263\text{–}267, 269, 271, 274, 275, 279, 283, 286, 287, 289\text{–}291, 294, 295, 297, 298.$$

In addition, there are no KM-logarithms of length k for

$$k = 184, 234, 236.$$

In addition, there are no special KM-logarithms of length k for

$$k = 4, 12, 60, 180, 182, 190, 196, 222, 238, 268, 276, 282, 292.$$

Logarithms: computational results

Let us call a logarithm **sporadic** if it does not come from $k+1$ or $2k+1$ being prime.

Logarithms: computational results

Let us call a logarithm **sporadic** if it does not come from $k+1$ or $2k+1$ being prime.

The values of k for which there are only sporadic logarithms seem increasingly rare as k grows.

Logarithms: computational results

Let us call a logarithm **sporadic** if it does not come from $k+1$ or $2k+1$ being prime.

The values of k for which there are only sporadic logarithms seem increasingly rare as k grows.

For $k \geq 200$, the only known cases are

$$k = 201, 202, 203, 206, 207, 213, 223, 225, 234, 236, 237, 241, 272, 277.$$

Logarithms: computational results

Let us call a logarithm **sporadic** if it does not come from $k+1$ or $2k+1$ being prime.

The values of k for which there are only sporadic logarithms seem increasingly rare as k grows.

For $k \geq 200$, the only known cases are

$$k = 201, 202, 203, 206, 207, 213, 223, 225, 234, 236, 237, 241, 272, 277.$$

News flash: there is also a logarithm of length 342.

Logarithms: computational results

Let us call a logarithm **sporadic** if it does not come from $k + 1$ or $2k + 1$ being prime.

The values of k for which there are only sporadic logarithms seem increasingly rare as k grows.

For $k \geq 200$, the only known cases are

$$k = 201, 202, 203, 206, 207, 213, 223, 225, 234, 236, 237, 241, 272, 277.$$

News flash: there is also a logarithm of length 342.

And one of length 360.

k-radius primes: density

Let N_k be the number of special KM-logarithms of length k.

k-radius primes: density

Let N_k be the number of special KM-logarithms of length k.

Define

$$c_k = \begin{cases} \dfrac{1}{\varphi(2k)} \cdot \dfrac{N_k}{k^{\pi(k)}} & \text{if } k \text{ is odd,} \\[2ex] \dfrac{1}{\varphi(2k)} \cdot \dfrac{N_k 2^{\omega(k/2)}}{k^{\pi(k)}} & \text{if } k \text{ is even.} \end{cases}$$

k-radius primes: density

Let N_k be the number of special KM-logarithms of length k.

Define

$$c_k = \begin{cases} \dfrac{1}{\varphi(2k)} \cdot \dfrac{N_k}{k^{\pi(k)}} & \text{if } k \text{ is odd,} \\[2ex] \dfrac{1}{\varphi(2k)} \cdot \dfrac{N_k 2^{\omega(k/2)}}{k^{\pi(k)}} & \text{if } k \text{ is even.} \end{cases}$$

Theorem (Blackburn, M [2012])

The number of k-radius primes below x is asymptotic to $c_k x/\log x$ (as $x \to \infty$).

Open problems

- Is the number of sporadic logarithms finite?

Open problems

- Is the number of sporadic logarithms finite? Is there one of length greater than ~~277~~ ~~342~~ 360?

Open problems

- Is the number of sporadic logarithms finite? Is there one of length greater than 360?

- Is the number of k for which there exist logarithms, but not KM-logarithms, finite?

Open problems

- Is the number of sporadic logarithms finite? Is there one of length greater than 360?

- Is the number of k for which there exist logarithms, but not KM-logarithms, finite?

- Is the number of k for which there exist logarithms, but not special KM-logarithms, infinite?

A logarithm of length 342

2	3	5	7	11	13	17	19	23	29
1	139	232	150	102	329	226	171	146	17

$\vdots$

277	281	283	293	307	311	313	317	331	337
298	309	313	314	319	326	327	339	340	341

A logarithm of length 342

1	2	3	4	5	6	7	8	9	10
0	1	139	2	232	140	150	3	278	233

11	12	13	14	15	16	17	18	19	20
102	141	329	151	29	4	226	279	171	234

⋮

333	334	335	336	337	338	339	340	341	342
323	268	159	293	341	317	134	118	63	108

A logarithm of length 360

2	3	5	7	11	13	17	19	23	29
2	125	194	273	141	37	191	292	349	324

$\vdots$

307	311	313	317	331	337	347	349	353	359
236	241	271	285	290	331	334	344	348	358

A logarithm of length 360

1	2	3	4	5	6	7	8	9	10
0	2	125	4	194	127	273	6	250	196

11	12	13	14	15	16	17	18	19	20
141	129	37	275	319	8	191	252	292	198

$\vdots$

351	352	353	354	355	356	357	358	359	360
52	151	348	110	139	299	229	1	358	90