Dirichlet convolution and Möbius inversion formula

Golovanov399

Moscow Institute of Physics and Technology

2021

Problem

Given $n \leq 10^5$ positive integers $a_1, \ldots, a_n$ $(1 \leq a_i \leq 10^6)$, and also number $m \leq 10^5$. For each i from 1 to m print the number of non-empty subsequences of $\{a_i\}_{i=1}^n$ with LCM equal to i, modulo $998\,244\,353$.

Problem

Given $n \leq 10^5$ positive integers $a_1, \ldots, a_n$ $(1 \leq a_i \leq 10^6)$, and also number $m \leq 10^5$. For each i from 1 to m print the number of non-empty subsequences of $\{a_i\}_{i=1}^n$ with LCM equal to i, modulo $998\,244\,353$.

Thoughts.

What does it mean that a subsequence has its LCM equal to, say, 12?

Problem

Given $n \leq 10^5$ positive integers $a_1, \ldots, a_n$ $(1 \leq a_i \leq 10^6)$, and also number $m \leq 10^5$. For each i from 1 to m print the number of non-empty subsequences of $\{a_i\}_{i=1}^n$ with LCM equal to i, modulo $998\,244\,353$.

Thoughts.

What does it mean that a subsequence has its LCM equal to, say, 12? It at least means that all its members are factors of 12, so a first approach would be the number of subsequences containing only factors of 12. If c_{12} is the number of factors of 12, then there are $2^{c_{12}} - 1$ such subsequences.

Problem

Given $n \leq 10^5$ positive integers $a_1, \ldots, a_n$ ($1 \leq a_i \leq 10^6$), and also number $m \leq 10^5$. For each i from 1 to m print the number of non-empty subsequences of $\{a_i\}_{i=1}^n$ with LCM equal to i, modulo $998\,244\,353$.

Thoughts.

What does it mean that a subsequence has its LCM equal to, say, 12? It at least means that all its members are factors of 12, so a first approach would be the number of subsequences containing only factors of 12. If c_{12} is the number of factors of 12, then there are $2^{c_{12}} - 1$ such subsequences. However, we need to exclude all subsets of factors of 6, as their LCM is at most 6; the same about 4. Let's adjust the answer: $2^{c_{12}} - 2^{c_6} - 2^{c_4} + 1$.

Problem

Given $n \leq 10^5$ positive integers $a_1, \ldots, a_n$ ($1 \leq a_i \leq 10^6$), and also number $m \leq 10^5$. For each i from 1 to m print the number of non-empty subsequences of $\{a_i\}_{i=1}^n$ with LCM equal to i, modulo $998\,244\,353$.

Thoughts.

What does it mean that a subsequence has its LCM equal to, say, 12? It at least means that all its members are factors of 12, so a first approach would be the number of subsequences containing only factors of 12. If c_{12} is the number of factors of 12, then there are $2^{c_{12}} - 1$ such subsequences. However, we need to exclude all subsets of factors of 6, as their LCM is at most 6; the same about 4. Let's adjust the answer: $2^{c_{12}} - 2^{c_6} - 2^{c_4} + 1$. But now each subsequence of factors of 2 (that is, subsequence containing only ones and twos) is added once and subtracted twice, so we need to add them again: $2^{c_{12}} - 2^{c_6} - 2^{c_4} + 2^{c_2}$.

Problem

Given $n \le 10^5$ positive integers $a_1, \ldots, a_n$ $(1 \le a_i \le 10^6)$, and also number $m \le 10^5$. For each i from 1 to m print the number of non-empty subsequences of $\{a_i\}_{i=1}^n$ with LCM equal to i, modulo $998\,244\,353$.

Thoughts.

What does it mean that a subsequence has its LCM equal to, say, 12? It at least means that all its members are factors of 12, so a first approach would be the number of subsequences containing only factors of 12. If c_{12} is the number of factors of 12, then there are $2^{c_{12}} - 1$ such subsequences. However, we need to exclude all subsets of factors of 6, as their LCM is at most 6; the same about 4. Let's adjust the answer: $2^{c_{12}} - 2^{c_6} - 2^{c_4} + 1$. But now each subsequence of factors of 2 (that is, subsequence containing only ones and twos) is added once and subtracted twice, so we need to add them again: $2^{c_{12}} - 2^{c_6} - 2^{c_4} + 2^{c_2}$. Did we take everything into account?.. □

Möbius inversion in a nutshell

$g(0)$	$g(1)$	$g(2)$	$g(3)$	$g(4)$	$g(5)$	$g(6)$	$g(7)$	$g(8)$	$g(9)$	$g(10)$

$g(n) = \sum_{i=0}^{n} f(i)$

Möbius inversion in a nutshell

$g(0)$	$g(1)$	$g(2)$	$g(3)$	$g(4)$	$g(5)$	$g(6)$	$g(7)$	$g(8)$	$g(9)$	$g(10)$

$$g(n) = \sum_{i=0}^{n} f(i)$$

$g(0)$	$g(1)$	$g(2)$	$g(3)$	$g(4)$	$g(5)$	$g(6)$	$g(7)$	$g(8)$	$g(9)$	$g(10)$

$$f(n) = g(n) - g(n-1)$$

Möbius inversion in a nutshell

$g(0,4)$	$g(1,4)$	$g(2,4)$	$g(3,4)$	$g(4,4)$	$g(5,4)$	$g(6,4)$	$g(7,4)$	$g(8,4)$	$g(9,4)$	$g(10,4)$
$g(0,3)$	$g(1,3)$	$g(2,3)$	$g(3,3)$	$g(4,3)$	$g(5,3)$	$g(6,3)$	$g(7,3)$	$g(8,3)$	$g(9,3)$	$g(10,3)$
$g(0,2)$	$g(1,2)$	$g(2,2)$	$g(3,2)$	$g(4,2)$	$g(5,2)$	$g(6,2)$	$g(7,2)$	$g(8,2)$	$g(9,2)$	$g(10,2)$
$g(0,1)$	$g(1,1)$	$g(2,1)$	$g(3,1)$	$g(4,1)$	$g(5,1)$	$g(6,1)$	$g(7,1)$	$g(8,1)$	$g(9,1)$	$g(10,1)$
$g(0,0)$	$g(1,0)$	$g(2,0)$	$g(3,0)$	$g(4,0)$	$g(5,0)$	$g(6,0)$	$g(7,0)$	$g(8,0)$	$g(9,0)$	$g(10,0)$

$g(n,m) = \sum_{i=0}^{n} \sum_{j=0}^{m} f(i,j)$

Möbius inversion in a nutshell

$g(0,4)$	$g(1,4)$	$g(2,4)$	$g(3,4)$	$g(4,4)$	$g(5,4)$	$g(6,4)$	$g(7,4)$	$g(8,4)$	$g(9,4)$	$g(10,4)$
$g(0,3)$	$g(1,3)$	$g(2,3)$	$g(3,3)$	$g(4,3)$	$g(5,3)$	$g(6,3)$	$g(7,3)$	$g(8,3)$	$g(9,3)$	$g(10,3)$
$g(0,2)$	$g(1,2)$	$g(2,2)$	$g(3,2)$	$g(4,2)$	$g(5,2)$	$g(6,2)$	$g(7,2)$	$g(8,2)$	$g(9,2)$	$g(10,2)$
$g(0,1)$	$g(1,1)$	$g(2,1)$	$g(3,1)$	$g(4,1)$	$g(5,1)$	$g(6,1)$	$g(7,1)$	$g(8,1)$	$g(9,1)$	$g(10,1)$
$g(0,0)$	$g(1,0)$	$g(2,0)$	$g(3,0)$	$g(4,0)$	$g(5,0)$	$g(6,0)$	$g(7,0)$	$g(8,0)$	$g(9,0)$	$g(10,0)$

$$f(n,m) = g(n,m) - g(n-1,m) - g(n,m-1) + g(n-1,m-1)$$

Möbius inversion in a nutshell

$g(2^0 3^4)$	$g(2^1 3^4)$	$g(2^2 3^4)$	$g(2^3 3^4)$	$g(2^4 3^4)$	$g(2^5 3^4)$	$g(2^6 3^4)$	$g(2^7 3^4)$	$g(2^8 3^4)$	$g(2^9 3^4)$	$g(2^{10} 3^4)$
$g(2^0 3^3)$	$g(2^1 3^3)$	$g(2^2 3^3)$	$g(2^3 3^3)$	$g(2^4 3^3)$	$g(2^5 3^3)$	$g(2^6 3^3)$	$g(2^7 3^3)$	$g(2^8 3^3)$	$g(2^9 3^3)$	$g(2^{10} 3^3)$
$g(2^0 3^2)$	$g(2^1 3^2)$	$g(2^2 3^2)$	$g(2^3 3^2)$	$g(2^4 3^2)$	$g(2^5 3^2)$	$g(2^6 3^2)$	$g(2^7 3^2)$	$g(2^8 3^2)$	$g(2^9 3^2)$	$g(2^{10} 3^2)$
$g(2^0 3^1)$	$g(2^1 3^1)$	$g(2^2 3^1)$	$g(2^3 3^1)$	$g(2^4 3^1)$	$g(2^5 3^1)$	$g(2^6 3^1)$	$g(2^7 3^1)$	$g(2^8 3^1)$	$g(2^9 3^1)$	$g(2^{10} 3^1)$
$g(2^0 3^0)$	$g(2^1 3^0)$	$g(2^2 3^0)$	$g(2^3 3^0)$	$g(2^4 3^0)$	$g(2^5 3^0)$	$g(2^6 3^0)$	$g(2^7 3^0)$	$g(2^8 3^0)$	$g(2^9 3^0)$	$g(2^{10} 3^0)$

$$g(2^n 3^m) = \sum_{i=0}^{n} \sum_{j=0}^{m} f(2^i 3^j)$$

$$f(2^n 3^m) = g(2^n 3^m) - g(2^{n-1} 3^m) - g(2^n 3^{m-1}) + g(2^{n-1} 3^{m-1})$$

Möbius inversion in a nutshell

$g(2^0 3^4)$	$g(2^1 3^4)$	$g(2^2 3^4)$	$g(2^3 3^4)$	$g(2^4 3^4)$	$g(2^5 3^4)$	$g(2^6 3^4)$	$g(2^7 3^4)$	$g(2^8 3^4)$	$g(2^9 3^4)$	$g(2^{10} 3^4)$
$g(2^0 3^3)$	$g(2^1 3^3)$	$g(2^2 3^3)$	$g(2^3 3^3)$	$g(2^4 3^3)$	$g(2^5 3^3)$	$g(2^6 3^3)$	$g(2^7 3^3)$	$g(2^8 3^3)$	$g(2^9 3^3)$	$g(2^{10} 3^3)$
$g(2^0 3^2)$	$g(2^1 3^2)$	$g(2^2 3^2)$	$g(2^3 3^2)$	$g(2^4 3^2)$	$g(2^5 3^2)$	$g(2^6 3^2)$	$g(2^7 3^2)$	$g(2^8 3^2)$	$g(2^9 3^2)$	$g(2^{10} 3^2)$
$g(2^0 3^1)$	$g(2^1 3^1)$	$g(2^2 3^1)$	$g(2^3 3^1)$	$g(2^4 3^1)$	$g(2^5 3^1)$	$g(2^6 3^1)$	$g(2^7 3^1)$	$g(2^8 3^1)$	$g(2^9 3^1)$	$g(2^{10} 3^1)$
$g(2^0 3^0)$	$g(2^1 3^0)$	$g(2^2 3^0)$	$g(2^3 3^0)$	$g(2^4 3^0)$	$g(2^5 3^0)$	$g(2^6 3^0)$	$g(2^7 3^0)$	$g(2^8 3^0)$	$g(2^9 3^0)$	$g(2^{10} 3^0)$

$$g(2^n 3^m) = \sum_{i=0}^{n} \sum_{j=0}^{m} f(2^i 3^j)$$

$$f(2^n 3^m) = g(2^n 3^m) - g(2^{n-1} 3^m) - g(2^n 3^{m-1}) + g(2^{n-1} 3^{m-1})$$

We are going to develop this theory and generalize it on "higher dimensions".

Convolutions in general

What is a convolution?

Convolutions in general

What is a convolution?
Some of them:

Convolutions in general

What is a convolution?
Some of them:

- Polynomial multiplication is a convolution: $(a_i), (b_i) \to (c_i)$, where
$$c_i = \sum_{j+k=i} a_j b_k.$$

Convolutions in general

What is a convolution?
Some of them:

- Polynomial multiplication is a convolution: $(a_i), (b_i) \to (c_i)$, where
$$c_i = \sum_{j+k=i} a_j b_k.$$
- Bitwise and convolution: $(a_i), (b_i) \to (c_i)$, where
$$c_i = \sum_{j \,\&\, k=i} a_j b_k.$$

Convolutions in general

What is a convolution?
Some of them:

- Polynomial multiplication is a convolution: $(a_i), (b_i) \to (c_i)$, where

$$c_i = \sum_{j+k=i} a_j b_k.$$

- Bitwise and convolution: $(a_i), (b_i) \to (c_i)$, where

$$c_i = \sum_{j \,\&\, k=i} a_j b_k.$$

- Bitwise xor convolution: $(a_i), (b_i) \to (c_i)$, where

$$c_i = \sum_{j \oplus k=i} a_j b_k.$$

Convolutions in general

What is a convolution?
Some of them:

- Polynomial multiplication is a convolution: $(a_i), (b_i) \to (c_i)$, where
$$c_i = \sum_{j+k=i} a_j b_k.$$
- Bitwise and convolution: $(a_i), (b_i) \to (c_i)$, where
$$c_i = \sum_{j \,\&\, k=i} a_j b_k.$$
- Bitwise xor convolution: $(a_i), (b_i) \to (c_i)$, where
$$c_i = \sum_{j \oplus k=i} a_j b_k.$$
- etc.

Convolutions in general

If we generalize this:
If we have two functions $f, g\colon (G, \cdot) \to \mathbb{R}$ (G is a set, and $\cdot$ is an operation over this set. It can be $(\mathbb{Z}_{\geq 0}, +)$, $(\mathbb{Z}_{2^k}, \oplus)$ or something else. $\mathbb{R}$ can be replaced by $\mathbb{Z}_{998\,244\,353}$ or smth), then

$$(f * g)(i) \overset{\text{def}}{=} \sum_{j \cdot k = i} f(j)g(k).$$

Convolutions in general

Indeed,

Convolutions in general

Indeed,

- If $(G, \cdot) = (\mathbb{Z}_{\geq 0}, +)$, then

$$(f * g)(i) = \sum_{j+k=i} f(j)g(k).$$

Convolutions in general

Indeed,

- If $(G, \cdot) = (\mathbb{Z}_{\geq 0}, +)$, then

$$(f * g)(i) = \sum_{j+k=i} f(j)g(k).$$

- If $(G, \cdot) = (\mathbb{Z}_{2^k}, \,\&\,)$, then

$$(f * g)(i) = \sum_{j \,\&\, k=i} f(j)g(k).$$

Convolutions in general

Indeed,

- If $(G, \cdot) = (\mathbb{Z}_{\geq 0}, +)$, then
$$(f * g)(i) = \sum_{j+k=i} f(j)g(k).$$
- If $(G, \cdot) = (\mathbb{Z}_{2^k}, \ \&\ )$, then
$$(f * g)(i) = \sum_{j \,\&\, k=i} f(j)g(k).$$
- If $(G, \cdot) = (\mathbb{Z}_{2^k}, \oplus)$, then
$$(f * g)(i) = \sum_{j \oplus k=i} f(j)g(k).$$

Dirichlet convolution

Definition

Dirichlet convolution of two functions $f, g : \mathbb{N} \to \mathbb{R}$

Dirichlet convolution

Definition

Dirichlet convolution of two functions $f, g : \mathbb{N} \to \mathbb{R}$ (or $\to \mathbb{Z}_{mod}$)

Dirichlet convolution

Definition

Dirichlet convolution of two functions $f, g : \mathbb{N} \to \mathbb{R}$ (or $\to \mathbb{Z}_{mod}$) is a convolution for $(G, \cdot) = (\mathbb{N}, \times)$:

Dirichlet convolution

Definition

Dirichlet convolution of two functions $f, g : \mathbb{N} \to \mathbb{R}$ (or $\to \mathbb{Z}_{mod}$) is a convolution for $(G, \cdot) = (\mathbb{N}, \times)$:

$$(f * g)(n) = \sum_{ab=n} f(a)g(b)$$

Dirichlet convolution

Definition

Dirichlet convolution of two functions $f, g : \mathbb{N} \to \mathbb{R}$ (or $\to \mathbb{Z}_{mod}$) is a convolution for $(G, \cdot) = (\mathbb{N}, \times)$:

$$(f * g)(n) = \sum_{ab=n} f(a)g(b) = \sum_{d|n} f(d)g\left(\frac{n}{d}\right).$$

Dirichlet convolution

Definition

Dirichlet convolution of two functions $f, g : \mathbb{N} \to \mathbb{R}$ (or $\to \mathbb{Z}_{mod}$) is a convolution for $(G, \cdot) = (\mathbb{N}, \times)$:

$$(f * g)(n) = \sum_{ab=n} f(a)g(b) = \sum_{d|n} f(d)g\left(\frac{n}{d}\right).$$

From now on we assume that $*$ is the Dirichlet convolution.

Which functions may be useful?

The following functions are usually considered when dealing with the convolution/inversion formula:

Which functions may be useful?

The following functions are usually considered when dealing with the convolution/inversion formula:

- $id(n) \equiv n$,

Which functions may be useful?

The following functions are usually considered when dealing with the convolution/inversion formula:

- $id(n) \equiv n$,
- $\mathbf{1}(n) \equiv 1$,

Which functions may be useful?

The following functions are usually considered when dealing with the convolution/inversion formula:

- $id(n) \equiv n$,
- $\mathbf{1}(n) \equiv 1$,
- $\mathbf{0}(n) \equiv 0$,

Which functions may be useful?

The following functions are usually considered when dealing with the convolution/inversion formula:

- $id(n) \equiv n$,
- $\mathbf{1}(n) \equiv 1$,
- $\mathbf{0}(n) \equiv 0$,
- $\sigma_0(n) \equiv \#\{d \mid n\}$

Which functions may be useful?

The following functions are usually considered when dealing with the convolution/inversion formula:

- $id(n) \equiv n$,
- $\mathbf{1}(n) \equiv 1$,
- $\mathbf{0}(n) \equiv 0$,
- $\sigma_0(n) \equiv \#\{d \mid n\} = \sum_{d|n} d^0$,
- $\sigma_1(n) \equiv \sum_{d|n} d$,

Which functions may be useful?

The following functions are usually considered when dealing with the convolution/inversion formula:

- $id(n) \equiv n$,
- $\mathbf{1}(n) \equiv 1$,
- $\mathbf{0}(n) \equiv 0$,
- $\sigma_0(n) \equiv \#\{d \mid n\} = \sum_{d|n} d^0$,
- $\sigma_1(n) \equiv \sum_{d|n} d$,
- $\chi_1(n) \equiv [n = 1] = \begin{cases} 1, & n = 1, \\ 0, & \text{otherwise.} \end{cases}$

Which functions may be useful?

The following functions are usually considered when dealing with the convolution/inversion formula:

- $id(n) \equiv n$,
- $\mathbf{1}(n) \equiv 1$,
- $\mathbf{0}(n) \equiv 0$,
- $\sigma_0(n) \equiv \#\{d \mid n\} = \sum_{d|n} d^0$,
- $\sigma_1(n) \equiv \sum_{d|n} d$,
- $\chi_1(n) \equiv [n = 1] = \begin{cases} 1, & n = 1, \\ 0, & \text{otherwise.} \end{cases}$
- Euler totient function:

$$\varphi(n) \equiv \#\{a \leq n : \gcd(a, n) = 1)\},$$

- Möbius function:

$$\mu(n) \equiv \begin{cases} 0, & n \text{ is not squarefree}, \\ (-1)^k, & n \text{ has } k \text{ distinct prime factors.} \end{cases}$$

Properties

- $f * g = g * f$,

Properties

- $f * g = g * f$,
- $(f * g) * h = f * (g * h)$,

Properties

- $f * g = g * f$,
- $(f * g) * h = f * (g * h)$,
- $f * (g + h) = f * g + f * h$,

Properties

- $f * g = g * f$,
- $(f * g) * h = f * (g * h)$,
- $f * (g + h) = f * g + f * h$,
- $f * \chi_1 = f$,

Properties

- $f * g = g * f$,
- $(f * g) * h = f * (g * h)$,
- $f * (g + h) = f * g + f * h$,
- $f * \chi_1 = f$,
- $f * \mathbf{0} = \mathbf{0}$.

Properties

- $f * g = g * f$,
- $(f * g) * h = f * (g * h)$,
- $f * (g + h) = f * g + f * h$,
- $f * \chi_1 = f$,
- $f * \mathbf{0} = \mathbf{0}$.

One could say that such functions represent a ring (which is called *Dirichlet ring*). If you do not know what a ring is, never mind. Basically you can do to these functions about everything that you can do, say, to remainders modulo 10. In particular, you can find an inverse of some (not all) functions.

Inverse

Definition

An *inverse* of a function f is such function g that $f * g = \chi_1$. We denote g by f^{-1}.

Inverse

Definition

An *inverse* of a function f is such function g that $f * g = \chi_1$. We denote g by f^{-1}.

It can be shown that a function f has the (unique) inverse if and only if $f(1) \neq 0$. Basically in this case you can determine $f^{-1}(1)$, then $f^{-1}(2)$, and so on. Let's practice.

Inverses of some functions

- If $g = \chi_1^{-1}$ then $g(1) = 1$,

Inverses of some functions

- If $g = \chi_1^{-1}$ then $g(1) = 1$, $g(2) = (0 - g(1)\chi_1(2))/\chi_1(1) = 0$,

Inverses of some functions

- If $g = \chi_1^{-1}$ then $g(1) = 1$, $g(2) = (0 - g(1)\chi_1(2))/\chi_1(1) = 0$, $\ldots$, $g(n) = 0$, so $g = \chi_1$.

Inverses of some functions

- If $g = \chi_1^{-1}$ then $g(1) = 1$, $g(2) = (0 - g(1)\chi_1(2))/\chi_1(1) = 0$, $\dots$, $g(n) = 0$, so $g = \chi_1$.
- $\mathbf{0}$ does not have an inverse, since $\mathbf{0}(1) = 0$.

Inverses of some functions

- If $g = \chi_1^{-1}$ then $g(1) = 1$, $g(2) = (0 - g(1)\chi_1(2))/\chi_1(1) = 0$, $\ldots$, $g(n) = 0$, so $g = \chi_1$.
- $\mathbf{0}$ does not have an inverse, since $\mathbf{0}(1) = 0$.
- id^{-1}? σ_0^{-1}? σ_1^{-1}? $\mathbf{1}^{-1}$? φ^{-1}? μ^{-1}?

Multiplicative functions

Definition

A function f is *multiplicative*, if for every $a, b \in \mathbb{N}$ s. t. $\gcd(a, b) = 1$ one has $f(ab) = f(a)f(b)$.

Multiplicative functions

Definition

A function f is *multiplicative*, if for every $a, b \in \mathbb{N}$ s. t. $\gcd(a, b) = 1$ one has $f(ab) = f(a)f(b)$. Essentially it means that if $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ then $f(n) = f(p_1^{\alpha_1}) \cdots f(p_k^{\alpha_k})$.

Multiplicative functions

Definition

A function f is *multiplicative*, if for every $a, b \in \mathbb{N}$ s. t. $\gcd(a, b) = 1$ one has $f(ab) = f(a)f(b)$. Essentially it means that if $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ then $f(n) = f(p_1^{\alpha_1}) \cdots f(p_k^{\alpha_k})$.

It turns out that all these functions are multiplicative:

Multiplicative functions

Definition

A function f is *multiplicative*, if for every $a, b \in \mathbb{N}$ s. t. $\gcd(a, b) = 1$ one has $f(ab) = f(a)f(b)$. Essentially it means that if $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ then $f(n) = f(p_1^{\alpha_1}) \cdots f(p_k^{\alpha_k})$.

It turns out that all these functions are multiplicative:

- $id(ab) = ab = id(a)id(b)$.

Multiplicative functions

Definition

A function f is *multiplicative*, if for every $a, b \in \mathbb{N}$ s. t. $\gcd(a, b) = 1$ one has $f(ab) = f(a)f(b)$. Essentially it means that if $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ then $f(n) = f(p_1^{\alpha_1}) \cdots f(p_k^{\alpha_k})$.

It turns out that all these functions are multiplicative:

- $id(ab) = ab = id(a)id(b)$.
- $\sigma_0(p_1^{\alpha_1} \cdots p_k^{\alpha_k}) = (\alpha_1 + 1) \cdots (\alpha_k + 1) = \sigma_0(p_1^{\alpha_1}) \cdots \sigma_0(p_k^{\alpha_k})$.

Multiplicative functions

Definition

A function f is *multiplicative*, if for every $a, b \in \mathbb{N}$ s. t. $\gcd(a, b) = 1$ one has $f(ab) = f(a)f(b)$. Essentially it means that if $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ then $f(n) = f(p_1^{\alpha_1}) \cdots f(p_k^{\alpha_k})$.

It turns out that all these functions are multiplicative:

- $id(ab) = ab = id(a)id(b)$.
- $\sigma_0(p_1^{\alpha_1} \cdots p_k^{\alpha_k}) = (\alpha_1 + 1) \cdots (\alpha_k + 1) = \sigma_0(p_1^{\alpha_1}) \cdots \sigma_0(p_k^{\alpha_k})$.
- $\sigma_1(p_1^{\alpha_1} \cdots p_k^{\alpha_k}) = \frac{p_1^{\alpha_1+1}-1}{p_1-1} \cdots \frac{p_1^{\alpha_k+1}-1}{p_k-1} = \sigma_1(p_1^{\alpha_1}) \cdots \sigma_1(p_k^{\alpha_k})$.

Multiplicative functions

Definition

A function f is *multiplicative*, if for every $a, b \in \mathbb{N}$ s. t. $\gcd(a,b) = 1$ one has $f(ab) = f(a)f(b)$. Essentially it means that if $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ then $f(n) = f(p_1^{\alpha_1}) \cdots f(p_k^{\alpha_k})$.

It turns out that all these functions are multiplicative:

- $id(ab) = ab = id(a)id(b)$.
- $\sigma_0(p_1^{\alpha_1} \cdots p_k^{\alpha_k}) = (\alpha_1 + 1) \cdots (\alpha_k + 1) = \sigma_0(p_1^{\alpha_1}) \cdots \sigma_0(p_k^{\alpha_k})$.
- $\sigma_1(p_1^{\alpha_1} \cdots p_k^{\alpha_k}) = \frac{p_1^{\alpha_1+1}-1}{p_1-1} \cdots \frac{p_1^{\alpha_k+1}-1}{p_k-1} = \sigma_1(p_1^{\alpha_1}) \cdots \sigma_1(p_k^{\alpha_k})$.
- $\varphi(p_1^{\alpha_1} \cdots p_k^{\alpha_k}) = (p_1^{\alpha_1} - p_1^{\alpha_1-1}) \cdots (p_k^{\alpha_k} - p_k^{\alpha_k-1}) = \varphi(p_1^{\alpha_1}) \cdots \varphi(p_k^{\alpha_k})$.

Multiplicative functions

Definition

A function f is *multiplicative*, if for every $a, b \in \mathbb{N}$ s. t. $\gcd(a, b) = 1$ one has $f(ab) = f(a)f(b)$. Essentially it means that if $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ then $f(n) = f(p_1^{\alpha_1}) \cdots f(p_k^{\alpha_k})$.

It turns out that all these functions are multiplicative:

- $id(ab) = ab = id(a)id(b)$.
- $\sigma_0(p_1^{\alpha_1} \cdots p_k^{\alpha_k}) = (\alpha_1 + 1) \cdots (\alpha_k + 1) = \sigma_0(p_1^{\alpha_1}) \cdots \sigma_0(p_k^{\alpha_k})$.
- $\sigma_1(p_1^{\alpha_1} \cdots p_k^{\alpha_k}) = \frac{p_1^{\alpha_1+1}-1}{p_1-1} \cdots \frac{p_1^{\alpha_k+1}-1}{p_k-1} = \sigma_1(p_1^{\alpha_1}) \cdots \sigma_1(p_k^{\alpha_k})$.
- $\varphi(p_1^{\alpha_1} \cdots p_k^{\alpha_k}) = (p_1^{\alpha_1} - p_1^{\alpha_1-1}) \cdots (p_k^{\alpha_k} - p_k^{\alpha_k-1}) = \varphi(p_1^{\alpha_1}) \cdots \varphi(p_k^{\alpha_k})$.
- $\mu(p_1^{\alpha_1} \cdots p_k^{\alpha_k}) = (-1)^k[\alpha_1 = 1] \cdots [\alpha_k = 1] = \mu(p_1^{\alpha_1}) \cdots \mu(p_k^{\alpha_k})$.

Inverses for multiplicative functions

It can be shown (exercise for the reader) that the inverse of a multiplicative function is also multiplicative.

Inverses for multiplicative functions

It can be shown (exercise for the reader) that the inverse of a multiplicative function is also multiplicative. This means that it makes sense to find inverses only at prime powers: if $g = f^{-1}$ then we can fix a prime p and find

Inverses for multiplicative functions

It can be shown (exercise for the reader) that the inverse of a multiplicative function is also multiplicative. This means that it makes sense to find inverses only at prime powers: if $g = f^{-1}$ then we can fix a prime p and find

$$g(1) = 1/f(1),$$

Inverses for multiplicative functions

It can be shown (exercise for the reader) that the inverse of a multiplicative function is also multiplicative. This means that it makes sense to find inverses only at prime powers: if $g = f^{-1}$ then we can fix a prime p and find

$$g(1) = 1/f(1),$$

$$g(p) = -(g(1)f(p))/f(1),$$

Inverses for multiplicative functions

It can be shown (exercise for the reader) that the inverse of a multiplicative function is also multiplicative. This means that it makes sense to find inverses only at prime powers: if $g = f^{-1}$ then we can fix a prime p and find

$$g(1) = 1/f(1),$$

$$g(p) = -(g(1)f(p))/f(1),$$

$$\dots$$

$$g(p^k) = -(g(1)f(p^k) + \ldots + g(p^{k-1})f(p))/f(1).$$

Finding inverses for the remaining functions

- If $g = id^{-1}$, then $g(1) = 1$,

Finding inverses for the remaining functions

- If $g = id^{-1}$, then $g(1) = 1$, $g(p) = -p$,

Finding inverses for the remaining functions

- If $g = id^{-1}$, then $g(1) = 1$, $g(p) = -p$, $g(p^2) = -p^2 + p^2 = 0$,

Finding inverses for the remaining functions

- If $g = id^{-1}$, then $g(1) = 1$, $g(p) = -p$, $g(p^2) = -p^2 + p^2 = 0$, $g(p^3) = -p^3 + p^3 = 0$, and so on. Thus, $id^{-1}(n) = n \cdot \mu(n)$.

Finding inverses for the remaining functions

- If $g = id^{-1}$, then $g(1) = 1$, $g(p) = -p$, $g(p^2) = -p^2 + p^2 = 0$, $g(p^3) = -p^3 + p^3 = 0$, and so on. Thus, $id^{-1}(n) = n \cdot \mu(n)$.
- If $g = \sigma_0^{-1}$, then $g(1) = 1$,

Finding inverses for the remaining functions

- If $g = id^{-1}$, then $g(1) = 1$, $g(p) = -p$, $g(p^2) = -p^2 + p^2 = 0$, $g(p^3) = -p^3 + p^3 = 0$, and so on. Thus, $id^{-1}(n) = n \cdot \mu(n)$.
- If $g = \sigma_0^{-1}$, then $g(1) = 1$, $g(p) = -2$,

Finding inverses for the remaining functions

- If $g = id^{-1}$, then $g(1) = 1$, $g(p) = -p$, $g(p^2) = -p^2 + p^2 = 0$, $g(p^3) = -p^3 + p^3 = 0$, and so on. Thus, $id^{-1}(n) = n \cdot \mu(n)$.
- If $g = \sigma_0^{-1}$, then $g(1) = 1$, $g(p) = -2$, $g(p^2) = -3 + 4 = 1$,

Finding inverses for the remaining functions

- If $g = id^{-1}$, then $g(1) = 1$, $g(p) = -p$, $g(p^2) = -p^2 + p^2 = 0$, $g(p^3) = -p^3 + p^3 = 0$, and so on. Thus, $id^{-1}(n) = n \cdot \mu(n)$.
- If $g = \sigma_0^{-1}$, then $g(1) = 1$, $g(p) = -2$, $g(p^2) = -3 + 4 = 1$, $g(p^3) = -4 + 6 - 2 = 0$,

Finding inverses for the remaining functions

- If $g = id^{-1}$, then $g(1) = 1$, $g(p) = -p$, $g(p^2) = -p^2 + p^2 = 0$, $g(p^3) = -p^3 + p^3 = 0$, and so on. Thus, $id^{-1}(n) = n \cdot \mu(n)$.
- If $g = \sigma_0^{-1}$, then $g(1) = 1$, $g(p) = -2$, $g(p^2) = -3 + 4 = 1$, $g(p^3) = -4 + 6 - 2 = 0$, $g(p^4) = -5 + 8 - 3 = 0$, and so on.

Finding inverses for the remaining functions

- If $g = id^{-1}$, then $g(1) = 1$, $g(p) = -p$, $g(p^2) = -p^2 + p^2 = 0$, $g(p^3) = -p^3 + p^3 = 0$, and so on. Thus, $id^{-1}(n) = n \cdot \mu(n)$.
- If $g = \sigma_0^{-1}$, then $g(1) = 1$, $g(p) = -2$, $g(p^2) = -3 + 4 = 1$, $g(p^3) = -4 + 6 - 2 = 0$, $g(p^4) = -5 + 8 - 3 = 0$, and so on.
- We skip σ_1^{-1}. You can practice on it yourself, though.

Finding inverses for the remaining functions

- If $g = id^{-1}$, then $g(1) = 1$, $g(p) = -p$, $g(p^2) = -p^2 + p^2 = 0$, $g(p^3) = -p^3 + p^3 = 0$, and so on. Thus, $id^{-1}(n) = n \cdot \mu(n)$.
- If $g = \sigma_0^{-1}$, then $g(1) = 1$, $g(p) = -2$, $g(p^2) = -3 + 4 = 1$, $g(p^3) = -4 + 6 - 2 = 0$, $g(p^4) = -5 + 8 - 3 = 0$, and so on.
- We skip σ_1^{-1}. You can practice on it yourself, though.
- If $g = \mathbf{1}^{-1}$, then $g(1) = 1$,

Finding inverses for the remaining functions

- If $g = id^{-1}$, then $g(1) = 1$, $g(p) = -p$, $g(p^2) = -p^2 + p^2 = 0$, $g(p^3) = -p^3 + p^3 = 0$, and so on. Thus, $id^{-1}(n) = n \cdot \mu(n)$.
- If $g = \sigma_0^{-1}$, then $g(1) = 1$, $g(p) = -2$, $g(p^2) = -3 + 4 = 1$, $g(p^3) = -4 + 6 - 2 = 0$, $g(p^4) = -5 + 8 - 3 = 0$, and so on.
- We skip σ_1^{-1}. You can practice on it yourself, though.
- If $g = \mathbf{1}^{-1}$, then $g(1) = 1$, $g(p) = -1$,

Finding inverses for the remaining functions

- If $g = id^{-1}$, then $g(1) = 1$, $g(p) = -p$, $g(p^2) = -p^2 + p^2 = 0$, $g(p^3) = -p^3 + p^3 = 0$, and so on. Thus, $id^{-1}(n) = n \cdot \mu(n)$.
- If $g = \sigma_0^{-1}$, then $g(1) = 1$, $g(p) = -2$, $g(p^2) = -3 + 4 = 1$, $g(p^3) = -4 + 6 - 2 = 0$, $g(p^4) = -5 + 8 - 3 = 0$, and so on.
- We skip σ_1^{-1}. You can practice on it yourself, though.
- If $g = \mathbf{1}^{-1}$, then $g(1) = 1$, $g(p) = -1$, $g(p^2) = -1 + 1 = 0$,

Finding inverses for the remaining functions

- If $g = id^{-1}$, then $g(1) = 1$, $g(p) = -p$, $g(p^2) = -p^2 + p^2 = 0$, $g(p^3) = -p^3 + p^3 = 0$, and so on. Thus, $id^{-1}(n) = n \cdot \mu(n)$.
- If $g = \sigma_0^{-1}$, then $g(1) = 1$, $g(p) = -2$, $g(p^2) = -3 + 4 = 1$, $g(p^3) = -4 + 6 - 2 = 0$, $g(p^4) = -5 + 8 - 3 = 0$, and so on.
- We skip σ_1^{-1}. You can practice on it yourself, though.
- If $g = \mathbf{1}^{-1}$, then $g(1) = 1$, $g(p) = -1$, $g(p^2) = -1 + 1 = 0$, $g(p^3) = -1 + 1 = 0$, and so on. Thus, $\mathbf{1}^{-1} = \mu$.

Finding inverses for the remaining functions

- If $g = id^{-1}$, then $g(1) = 1$, $g(p) = -p$, $g(p^2) = -p^2 + p^2 = 0$, $g(p^3) = -p^3 + p^3 = 0$, and so on. Thus, $id^{-1}(n) = n \cdot \mu(n)$.
- If $g = \sigma_0^{-1}$, then $g(1) = 1$, $g(p) = -2$, $g(p^2) = -3 + 4 = 1$, $g(p^3) = -4 + 6 - 2 = 0$, $g(p^4) = -5 + 8 - 3 = 0$, and so on.
- We skip σ_1^{-1}. You can practice on it yourself, though.
- If $g = \mathbf{1}^{-1}$, then $g(1) = 1$, $g(p) = -1$, $g(p^2) = -1 + 1 = 0$, $g(p^3) = -1 + 1 = 0$, and so on. Thus, $\mathbf{1}^{-1} = \mu$.
- This also means that $\mu^{-1} = \mathbf{1}$.

Why did I choose to attend this lecture

Fun fact: if $f = g * \mathbf{1}$ then

$$g = g * \chi_1 = g * (\mathbf{1} * \mu) = (g * \mathbf{1}) * \mu = f * \mu.$$

Why did I choose to attend this lecture

Fun fact: if $f = g * \mathbf{1}$ then

$$g = g * \chi_1 = g * (\mathbf{1} * \mu) = (g * \mathbf{1}) * \mu = f * \mu.$$

In human language: if $f(n) = \sum_{d|n} g(d)$ for all n, then $g(n) = \sum_{d|n} f(d)\mu\left(\frac{n}{d}\right)$ for all n.

Why did I choose to attend this lecture

Fun fact: if $f = g * \mathbf{1}$ then

$$g = g * \chi_1 = g * (\mathbf{1} * \mu) = (g * \mathbf{1}) * \mu = f * \mu.$$

In human language: if $f(n) = \sum_{d|n} g(d)$ for all n, then $g(n) = \sum_{d|n} f(d)\mu\left(\frac{n}{d}\right)$ for all n. This fact is called *Möbius inversion formula*.

Why did I choose to attend this lecture

Fun fact: if $f = g * \mathbf{1}$ then

$$g = g * \chi_1 = g * (\mathbf{1} * \mu) = (g * \mathbf{1}) * \mu = f * \mu.$$

In human language: if $f(n) = \sum_{d|n} g(d)$ for all n, then $g(n) = \sum_{d|n} f(d)\mu\left(\frac{n}{d}\right)$ for all n. This fact is called *Möbius inversion formula*.
This formula can be applied to whatever function is derived from the statement, not necessarily from the list above.

Problem

Given $n \leq 10^5$ positive integers $a_1, \ldots, a_n$ $(1 \leq a_i \leq 10^6)$, and also number $m \leq 10^5$. For each i from 1 to m print the number of non-empty subsequences of $\{a_i\}_{i=1}^n$ with LCM equal to i, modulo $998\,244\,353$.

Solution.

Let $f(d)$ be the number of subsequences where all members are factors of d.

Problem

Given $n \le 10^5$ positive integers $a_1, \ldots, a_n$ $(1 \le a_i \le 10^6)$, and also number $m \le 10^5$. For each i from 1 to m print the number of non-empty subsequences of $\{a_i\}_{i=1}^n$ with LCM equal to i, modulo $998\,244\,353$.

Solution.

Let $f(d)$ be the number of subsequences where all members are factors of d. Let $g(d)$ be the number of all subsequences with $\mathrm{LCM} = d$.

Problem

Given $n \leq 10^5$ positive integers $a_1, \ldots, a_n$ ($1 \leq a_i \leq 10^6$), and also number $m \leq 10^5$. For each i from 1 to m print the number of non-empty subsequences of $\{a_i\}_{i=1}^n$ with LCM equal to i, modulo $998\,244\,353$.

Solution.

Let $f(d)$ be the number of subsequences where all members are factors of d. Let $g(d)$ be the number of all subsequences with $\mathrm{LCM} = d$. One can see that:

$$\forall n \quad f(n) = \sum_{d|n} g(d),$$

Problem

Given $n \le 10^5$ positive integers $a_1, \ldots, a_n$ $(1 \le a_i \le 10^6)$, and also number $m \le 10^5$. For each i from 1 to m print the number of non-empty subsequences of $\{a_i\}_{i=1}^n$ with LCM equal to i, modulo $998\,244\,353$.

Solution.

Let $f(d)$ be the number of subsequences where all members are factors of d. Let $g(d)$ be the number of all subsequences with $\mathrm{LCM} = d$. One can see that:

$$\forall n \quad f(n) = \sum_{d|n} g(d),$$

so

$$\forall n \quad g(n) = \sum_{d|n} f(d)\mu\left(\frac{n}{d}\right).$$

Problem

Given $n \leq 10^5$ positive integers $a_1, \ldots, a_n$ ($1 \leq a_i \leq 10^6$), and also number $m \leq 10^5$. For each i from 1 to m print the number of non-empty subsequences of $\{a_i\}_{i=1}^n$ with LCM equal to i.

Solution.

Now we are facing three subproblems:

Problem

Given $n \leq 10^5$ positive integers $a_1, \ldots, a_n$ $(1 \leq a_i \leq 10^6)$, and also number $m \leq 10^5$. For each i from 1 to m print the number of non-empty subsequences of $\{a_i\}_{i=1}^n$ with LCM equal to i.

Solution.

Now we are facing three subproblems:

- How to find all $f(d)$?

Problem

Given $n \leq 10^5$ positive integers $a_1, \ldots, a_n$ ($1 \leq a_i \leq 10^6$), and also number $m \leq 10^5$. For each i from 1 to m print the number of non-empty subsequences of $\{a_i\}_{i=1}^{n}$ with LCM equal to i.

Solution.

Now we are facing three subproblems:

- How to find all $f(d)$?
- How to find all $\mu(d)$ (which is a more general question)?

Problem

Given $n \le 10^5$ positive integers $a_1, \ldots, a_n$ $(1 \le a_i \le 10^6)$, and also number $m \le 10^5$. For each i from 1 to m print the number of non-empty subsequences of $\{a_i\}_{i=1}^n$ with LCM equal to i.

Solution.

Now we are facing three subproblems:

- How to find all $f(d)$?
- How to find all $\mu(d)$ (which is a more general question)?
- How to compute all $g(d)$ efficiently using f and μ (or, in other words, how to find the convolution of these two functions)?

$\square$

How to find all $\mu(d)$?

The simplest way is to use the sieve of Eratosthenes: if you know $\texttt{min\_prime}[n]$ for every n,

How to find all $\mu(d)$?

The simplest way is to use the sieve of Eratosthenes: if you know $\texttt{min\_prime}[n]$ for every n, then

$$\mu(n) = \begin{cases} 1, & n = 1, \\ -\mu\left(\frac{n}{p}\right), & \texttt{min\_prime}[n] = p \neq \texttt{min\_prime}\left[\frac{n}{p}\right], \\ 0, & \text{otherwise.} \end{cases}$$

How to find all $\mu(d)$?

The simplest way is to use the sieve of Eratosthenes: if you know $\texttt{min\_prime}[n]$ for every n, then

$$\mu(n) = \begin{cases} 1, & n = 1, \\ -\mu\left(\frac{n}{p}\right), & \texttt{min\_prime}[n] = p \neq \texttt{min\_prime}\left[\frac{n}{p}\right], \\ 0, & \text{otherwise.} \end{cases}$$

```
mu[i] = 1;
for (int i = 2; i < MAXN; ++i) {
    if (int p = min_prime[i]; p != min_prime[i / p]) {
        mu[i] = -mu[i / p];
    } else {
        mu[i] = 0;
    }
}
```

Finding all $f(d)$ for $d \leq 10^6$

It should be clear that we do not actually care about the ordering of the input; what matters is how many times every number occurs. Denote by $\texttt{cnt}_i$ the number of occurrences of number i in the input.

Finding all $f(d)$ for $d \leq 10^6$

It should be clear that we do not actually care about the ordering of the input; what matters is how many times every number occurs. Denote by $\texttt{cnt}_i$ the number of occurrences of number i in the input. Then $f(n) = 2^{\sum_{d|n} \texttt{cnt}_d} - 1$.

Finding all $f(d)$ for $d \leq 10^6$

It should be clear that we do not actually care about the ordering of the input; what matters is how many times every number occurs. Denote by $\texttt{cnt}_i$ the number of occurrences of number i in the input. Then $f(n) = 2^{\sum_{d|n} \texttt{cnt}_d} - 1$. The following code:

```
for (int d = 1; d < MAXN; ++d) {
    for (int n = d; n < MAXN; n += d) {
        f[n] += cnt[d];
    }
    f[d] = binpow(2, f[d]) - 1;
}
```

works in $\dfrac{MAXN}{1} + \ldots + \dfrac{MAXN}{MAXN} = O(MAXN \log MAXN)$.

Again: code for $f = \text{cnt} * \mathbf{1}$

```
for (int d = 1; d < MAXN; ++d) {
    for (int n = d; n < MAXN; n += d) {
        f[n] += cnt[d];
    }
}
```

Code for $g = f * \mu$

```
for (int d = 1; d < MAXN; ++d) {
    for (int n = d; n < MAXN; n += d) {
        g[n] += f[d] * mu[n / d];
    }
}
```

Code for arbitrary $h = f * g$

```
for (int d = 1; d < MAXN; ++d) {
    for (int n = d; n < MAXN; n += d) {
        h[n] += f[d] * g[n / d];
    }
}
```

Problem

Given $n \le 10^5$ positive integers $a_1, \ldots, a_n$ $(1 \le a_i \le 10^6)$, and also number $m \le 10^5$. For each i from 1 to m print the number of non-empty subsequences of $\{a_i\}_{i=1}^n$ with LCM equal to i, modulo $998\,244\,353$.

The rest of the problem is to calculate $2^{f(d)}$ for various d, which can be done either by binary multiplication, or by pre-calculating all powers of two ($f(d) \le n$ by definition). Thus the problem is solved in $O(10^6 \log 10^6)$.

Another setup

Suppose we have a function $\mathrm{func}: \mathcal{S} \to \mathbb{N}$ in the statement, and the question is "How many elements $s \in \mathcal{S}$ are there so that $\mathrm{func}(a) = 1$?".

Another setup

Suppose we have a function $\mathrm{func} : \mathcal{S} \to \mathbb{N}$ in the statement, and the question is "How many elements $s \in \mathcal{S}$ are there so that $\mathrm{func}(a) = 1$?". Assume that we can easily calculate, given d, for how many elements s one has $\mathrm{func}(a)$ is *divisible* by d.

Another setup

Suppose we have a function $\mathrm{func} : \mathcal{S} \to \mathbb{N}$ in the statement, and the question is "How many elements $s \in \mathcal{S}$ are there so that $\mathrm{func}(a) = 1$?". Assume that we can easily calculate, given d, for how many elements s one has $\mathrm{func}(a)$ is *divisible* by d. If $f(d) = \#\{s \in \mathcal{S} : \mathrm{func}(s) = d\}$ and $g(d) = \#\{s \in \mathcal{S} : d \mid \mathrm{func}(s)\}$, then, by definition, $g(d) = \sum_{i=1}^{\infty} f(di)$.

Another setup

Suppose we have a function $\mathrm{func}: \mathcal{S} \to \mathbb{N}$ in the statement, and the question is "How many elements $s \in \mathcal{S}$ are there so that $\mathrm{func}(a) = 1$?". Assume that we can easily calculate, given d, for how many elements s one has $\mathrm{func}(a)$ is *divisible* by d. If $f(d) = \#\{s \in \mathcal{S} : \mathrm{func}(s) = d\}$ and $g(d) = \#\{s \in \mathcal{S} : d \mid \mathrm{func}(s)\}$, then, by definition, $g(d) = \sum_{i=1}^{\infty} f(di)$. Note that:

$$\sum_{d=1}^{\infty} g(d)\mu(d)$$

Another setup

Suppose we have a function $\mathrm{func} : \mathcal{S} \to \mathbb{N}$ in the statement, and the question is "How many elements $s \in \mathcal{S}$ are there so that $\mathrm{func}(a) = 1$?". Assume that we can easily calculate, given d, for how many elements s one has $\mathrm{func}(a)$ is *divisible* by d. If $f(d) = \#\{s \in \mathcal{S} : \mathrm{func}(s) = d\}$ and $g(d) = \#\{s \in \mathcal{S} : d \mid \mathrm{func}(s)\}$, then, by definition, $g(d) = \sum_{i=1}^{\infty} f(di)$. Note that:

$$\sum_{d=1}^{\infty} g(d)\mu(d) = \sum_{d=1}^{\infty} \sum_{i=1}^{\infty} f(di)\mu(d)$$

Another setup

Suppose we have a function $\mathrm{func}: \mathcal{S} \to \mathbb{N}$ in the statement, and the question is "How many elements $s \in \mathcal{S}$ are there so that $\mathrm{func}(a) = 1$?". Assume that we can easily calculate, given d, for how many elements s one has $\mathrm{func}(a)$ is *divisible* by d. If $f(d) = \#\{s \in \mathcal{S} : \mathrm{func}(s) = d\}$ and $g(d) = \#\{s \in \mathcal{S} : d \mid \mathrm{func}(s)\}$, then, by definition, $g(d) = \sum_{i=1}^{\infty} f(di)$. Note that:

$$\sum_{d=1}^{\infty} g(d)\mu(d) = \sum_{d=1}^{\infty}\sum_{i=1}^{\infty} f(di)\mu(d) = \sum_{n=1}^{\infty} f(n) \sum_{d|n} \mu(d) = f(1).$$

Another setup

Suppose we have a function $\mathrm{func}: \mathcal{S} \to \mathbb{N}$ in the statement, and the question is "How many elements $s \in \mathcal{S}$ are there so that $\mathrm{func}(a) = 1$?". Assume that we can easily calculate, given d, for how many elements s one has $\mathrm{func}(a)$ is *divisible* by d. If $f(d) = \#\{s \in \mathcal{S} : \mathrm{func}(s) = d\}$ and $g(d) = \#\{s \in \mathcal{S} : d \mid \mathrm{func}(s)\}$, then, by definition, $g(d) = \sum_{i=1}^{\infty} f(di)$. Note that:

$$\sum_{d=1}^{\infty} g(d)\mu(d) = \sum_{d=1}^{\infty} \sum_{i=1}^{\infty} f(di)\mu(d) = \sum_{n=1}^{\infty} f(n) \sum_{d|n} \mu(d) = f(1).$$

Similarly, $f(d) = \sum_{i=1}^{\infty} g(di)\mu(i)$.

Problem 2

Given $n \leq 10^5$ positive integers $a_1, \ldots, a_n$ ($1 \leq a_i \leq 10^6$), and also number $m \leq 10^5$. For each i from 1 to m print the number of non-empty subsequences of $\{a_i\}_{i=1}^{n}$ with GCD equal to i, modulo $998\,244\,353$.

Problem 2

Given $n \leq 10^5$ positive integers $a_1, \ldots, a_n$ ($1 \leq a_i \leq 10^6$), and also number $m \leq 10^5$. For each i from 1 to m print the number of non-empty subsequences of $\{a_i\}_{i=1}^n$ with GCD equal to i, modulo $998\,244\,353$.

The solution if very similar to the previous one. We calculate $g(d)$ for each d, counting the number of subsequences of multiples of d (again, in $MAXN/1 + \ldots + MAXN/MAXN$).

Problem 2

Given $n \leq 10^5$ positive integers $a_1, \ldots, a_n$ $(1 \leq a_i \leq 10^6)$, and also number $m \leq 10^5$. For each i from 1 to m print the number of non-empty subsequences of $\{a_i\}_{i=1}^{n}$ with GCD equal to i, modulo $998\,244\,353$.

The solution if very similar to the previous one. We calculate $g(d)$ for each d, counting the number of subsequences of multiples of d (again, in $MAXN/1 + \ldots + MAXN/MAXN$). Then we accumulate the sum of $g(di)\mu(i)$, then we are done.

Sublinear summation

Suppose that we have a function $f(n)$. Denote $F(n) = \sum_{i=1}^{n} f(n)$. Our goal is to calculate $F(n)$ in $o(n)$.

Sublinear summation

Suppose that we have a function $f(n)$. Denote $F(n) = \sum_{i=1}^{n} f(n)$. Our goal is to calculate $F(n)$ in $o(n)$.
There are *good* functions, for which their prefix sum can be computed quickly (maybe in $O(1)$ or in $O(\log n)$). If f is such a function, then there is no problem.

Sublinear summation

Suppose that we have a function $f(n)$. Denote $F(n) = \sum_{i=1}^{n} f(n)$. Our goal is to calculate $F(n)$ in $o(n)$.

There are *good* functions, for which their prefix sum can be computed quickly (maybe in $O(1)$ or in $O(\log n)$). If f is such a function, then there is no problem. In other case, suppose that we have two other good functions g and h so that $f * g = h$. Define G and H accordingly.

Sublinear summation

Suppose that we have a function $f(n)$. Denote $F(n) = \sum_{i=1}^{n} f(n)$. Our goal is to calculate $F(n)$ in $o(n)$.
There are *good* functions, for which their prefix sum can be computed quickly (maybe in $O(1)$ or in $O(\log n)$). If f is such a function, then there is no problem. In other case, suppose that we have two other good functions g and h so that $f * g = h$. Define G and H accordingly. Also, for the sake of simplicity, assume that $g(1) = 1$ (most of the times g is multiplicative anyway).

Sublinear summation

Suppose that we have a function $f(n)$. Denote $F(n) = \sum_{i=1}^{n} f(n)$. Our goal is to calculate $F(n)$ in $o(n)$.

There are *good* functions, for which their prefix sum can be computed quickly (maybe in $O(1)$ or in $O(\log n)$). If f is such a function, then there is no problem. In other case, suppose that we have two other good functions g and h so that $f * g = h$. Define G and H accordingly. Also, for the sake of simplicity, assume that $g(1) = 1$ (most of the times g is multiplicative anyway).

We know that $h(n) = \sum_{d|n} f(d)g(n/d)$.

Sublinear summation

Suppose that we have a function $f(n)$. Denote $F(n) = \sum_{i=1}^{n} f(n)$. Our goal is to calculate $F(n)$ in $o(n)$.
There are *good* functions, for which their prefix sum can be computed quickly (maybe in $O(1)$ or in $O(\log n)$). If f is such a function, then there is no problem. In other case, suppose that we have two other good functions g and h so that $f * g = h$. Define G and H accordingly. Also, for the sake of simplicity, assume that $g(1) = 1$ (most of the times g is multiplicative anyway).
We know that $h(n) = \sum_{d|n} f(d)g(n/d)$. In other words,

$$h(n) = f(n) + \sum_{d|n,\, d>1} f\left(\frac{n}{d}\right) g(d)$$

$$\Rightarrow f(n) = h(n) - \sum_{d|n,\, d>1} f\left(\frac{n}{d}\right) g(d).$$

Sublinear summation

Suppose that we have a function $f(n)$. Denote $F(n) = \sum_{i=1}^{n} f(n)$. Our goal is to calculate $F(n)$ in $o(n)$.
There are *good* functions, for which their prefix sum can be computed quickly (maybe in $O(1)$ or in $O(\log n)$). If f is such a function, then there is no problem. In other case, suppose that we have two other good functions g and h so that $f * g = h$. Define G and H accordingly. Also, for the sake of simplicity, assume that $g(1) = 1$ (most of the times g is multiplicative anyway).
We know that $h(n) = \sum_{d|n} f(d)g(n/d)$. In other words,

$$h(n) = f(n) + \sum_{d|n,\, d>1} f\left(\frac{n}{d}\right) g(d)$$

$$\Rightarrow f(n) = h(n) - \sum_{d|n,\, d>1} f\left(\frac{n}{d}\right) g(d).$$

Sublinear summation

$$h(n) = f(n) + \sum_{d|n,\, d>1} f\left(\frac{n}{d}\right) g(d)$$

$$\Rightarrow f(n) = h(n) - \sum_{d|n,\, d>1} f\left(\frac{n}{d}\right) g(d).$$

Sublinear summation

$$h(n) = f(n) + \sum_{d|n,\, d>1} f\left(\frac{n}{d}\right) g(d)$$

$$\Rightarrow f(n) = h(n) - \sum_{d|n,\, d>1} f\left(\frac{n}{d}\right) g(d).$$

Let's sum it over n:

Sublinear summation

$$h(n) = f(n) + \sum_{d|n,\, d>1} f\left(\frac{n}{d}\right) g(d)$$

$$\Rightarrow f(n) = h(n) - \sum_{d|n,\, d>1} f\left(\frac{n}{d}\right) g(d).$$

Let's sum it over n:

$$F(n) = \sum_{k=1}^{n} f(k) = \sum_{k=1}^{n} \left(h(k) - \sum_{d|k,\, d>1} f\left(\frac{k}{d}\right) g(d) \right)$$

$$= H(n) - \sum_{k=1}^{n} \sum_{d|k,\, d>1} f\left(\frac{k}{d}\right) g(d) = H(n) - \sum_{d=2}^{n} g(d) \sum_{d|k} f\left(\frac{k}{d}\right)$$

$$= H(n) - \sum_{d=2}^{n} g(d) F\left(\left\lfloor \frac{n}{d} \right\rfloor\right).$$

Sublinear summation

$$F(n) = H(n) - \sum_{d=2}^{n} g(d) F\left(\left\lfloor \frac{n}{d} \right\rfloor\right).$$

Sublinear summation

$$F(n) = H(n) - \sum_{d=2}^{n} g(d) F\left(\left\lfloor \frac{n}{d} \right\rfloor\right).$$

So to find $F(n)$, we need to know all $F(\lfloor n/d \rfloor)$.

Sublinear summation

$$F(n) = H(n) - \sum_{d=2}^{n} g(d) F\left(\left\lfloor \frac{n}{d} \right\rfloor\right).$$

So to find $F(n)$, we need to know all $F(\lfloor n/d \rfloor)$. But if we do it recurrently, if, say, inside computation of $F(\lfloor n/a \rfloor)$ we need to know $F(\lfloor \lfloor n/a \rfloor / b \rfloor)$, then this is the same as $F(\lfloor n/ab \rfloor)$ (also exercise for the reader).

Sublinear summation

$$F(n) = H(n) - \sum_{d=2}^{n} g(d) F\left(\left\lfloor \frac{n}{d} \right\rfloor\right).$$

So to find $F(n)$, we need to know all $F(\lfloor n/d \rfloor)$. But if we do it recurrently, if, say, inside computation of $F(\lfloor n/a \rfloor)$ we need to know $F(\lfloor \lfloor n/a \rfloor / b \rfloor)$, then this is the same as $F(\lfloor n/ab \rfloor)$ (also exercise for the reader). Since there are about $2\sqrt{n}$ values of type $\lfloor n/d \rfloor$ (about $\sqrt{n}$ of them correspond to small d, about $\sqrt{d}$ of them correspond to small n/d), we can compute all of this for all these values in ascending order.

Sublinear summation

$$F(n) = H(n) - \sum_{d=2}^{n} g(d) F\left(\left\lfloor \frac{n}{d} \right\rfloor\right).$$

What remains is to determine for every value of $\lfloor n/d \rfloor$ the segment of d-s corresponding to this value.

Sublinear summation

$$F(n) = H(n) - \sum_{d=2}^{n} g(d) F\left(\left\lfloor \frac{n}{d} \right\rfloor\right).$$

What remains is to determine for every value of $\lfloor n/d \rfloor$ the segment of d-s corresponding to this value. We know that the largest value, $\lfloor n/2 \rfloor$, corresponds to a segment starting with 2. If the current value k is achieved for a segment starting with d, then this segment ends with $\left\lfloor \frac{n}{\left\lfloor \frac{n}{d} \right\rfloor} \right\rfloor$:

$$\left\lfloor \frac{n}{x} \right\rfloor = k \Leftrightarrow k \le \frac{n}{x} < k+1 \Leftrightarrow \frac{n}{k+1} < x \le \frac{n}{k}.$$

Sublinear summation

$$F(n) = H(n) - \sum_{d=2}^{n} g(d) F\left(\left\lfloor \frac{n}{d} \right\rfloor\right).$$

Then the following code works:

```
long long F(long long n) {
    long long ans = H(n);
    long long d = 2;
    while (d <= n) {
        long long right = n / (n / d);
        ans -= F_cached[n / k] * (G(right) - G(d - 1));
        d = right + 1;
    }
    return F_cached[n] = ans;
}
```

Sublinear summation?

Let's assume that both H and G can be computed in $O(1)$, also `F_cached` can be accessed in $O(1)$. Then the whole procedure works in the following time:

Sublinear summation?

Let's assume that both H and G can be computed in $O(1)$, also `F_cached` can be accessed in $O(1)$. Then the whole procedure works in the following time:

$$\sum_{k=1}^{\lfloor\sqrt{n}\rfloor} (T_F(k) + T_F(n/k)) \approx \int_1^{\sqrt{n}} \left(\sqrt{k} + \sqrt{\frac{n}{k}}\right) \mathrm{d}k$$

$$= \int_1^{\sqrt{n}} \left(k^{1/2} + \sqrt{n}k^{-1/2}\right) \mathrm{d}k = \left(\frac{2}{3}k^{3/2} + 2\sqrt{n}k^{1/2}\right)\Bigg|_1^{\sqrt{n}}$$

$$= O\left(n^{3/4}\right).$$

Even faster summation

Let $K > \sqrt{n}$ be some constant. If f is multiplicative, then we can compute its values up to K using the linear sieve of Eratosthenes, also computing the values of F up to K. Then the complexity becomes

$$
\begin{aligned}
K + \sum_{k=1}^{\lfloor n/K \rfloor} (T_F(n/k)) &\approx K + \int_1^{n/K} \sqrt{\frac{n}{k}}\,\mathrm{d}k \\
&= K + \int_1^{n/K} \sqrt{n} k^{-1/2}\,\mathrm{d}k = K + 2\sqrt{n} k^{1/2} \Big|_1^{n/K}.
\end{aligned}
$$

Even faster summation

Let $K > \sqrt{n}$ be some constant. If f is multiplicative, then we can compute its values up to K using the linear sieve of Eratosthenes, also computing the values of F up to K. Then the complexity becomes

$$K + \sum_{k=1}^{\lfloor n/K \rfloor} \left(T_F(n/k)\right) \approx K + \int_1^{n/K} \sqrt{\frac{n}{k}}\,\mathrm{d}k$$

$$= K + \int_1^{n/K} \sqrt{n}k^{-1/2}\,\mathrm{d}k = K + 2\sqrt{n}k^{1/2}\Big|_1^{n/K}.$$

If we assign $K = n^{2/3}$ then the complexity becomes $O(n^{2/3})$.

?