Тема I: Многочлены

§ 5. Неприводимые многочлены над полем вычетов

М.В.Волков

Уральский федеральный университет
Институт естественных наук и математики
кафедра алгебры и фундаментальной информатики

2021/2022 учебный год

Постановка задачи

Поле вычетов по простому модулю p – это поле $\mathbb{F}_p$, элементами которого служат числа $0, 1, \ldots, p-1$ (*вычеты*, т.е. остатки от деления на p).

Поле вычетов по простому модулю p – это поле $\mathbb{F}_p$, элементами которого служат числа $0, 1, \ldots, p-1$ (*вычеты*, т.е. остатки от деления на p). Операции в $\mathbb{F}_p$ определяются так: сумма (произведение) вычетов a и b – это остаток от деления на p обычной суммы (соответственно, обычного произведения) чисел a и b.

Поле вычетов по простому модулю p – это поле $\mathbb{F}_p$, элементами которого служат числа $0, 1, \dots, p-1$ (*вычеты*, т.е. остатки от деления на p). Операции в $\mathbb{F}_p$ определяются так: сумма (произведение) вычетов a и b – это остаток от деления на p обычной суммы (соответственно, обычного произведения) чисел a и b.

Неприводимые многочлены над полями вычетов имеют множество практических применений для передачи, хранения и защиты информации.

Поле вычетов по простому модулю p – это поле $\mathbb{F}_p$, элементами которого служат числа $0, 1, \ldots, p-1$ (*вычеты*, т.е. остатки от деления на p). Операции в $\mathbb{F}_p$ определяются так: сумма (произведение) вычетов a и b – это остаток от деления на p обычной суммы (соответственно, обычного произведения) чисел a и b.

Неприводимые многочлены над полями вычетов имеют множество практических применений для передачи, хранения и защиты информации.

Например, шифр «Кузнечик» (стандарт ГОСТ 34.12-2018, введен в действие в качестве стандарта Российской Федерации с 1 июня 2019 г.) использует неприводимый над $\mathbb{F}_2$ многочлен $x^8 + x^7 + x^6 + x + 1$.

Поле вычетов по простому модулю p – это поле $\mathbb{F}_p$, элементами которого служат числа $0, 1, \ldots, p-1$ (*вычеты*, т.е. остатки от деления на p). Операции в $\mathbb{F}_p$ определяются так: сумма (произведение) вычетов a и b – это остаток от деления на p обычной суммы (соответственно, обычного произведения) чисел a и b.

Неприводимые многочлены над полями вычетов имеют множество практических применений для передачи, хранения и защиты информации.

Например, шифр «Кузнечик» (стандарт ГОСТ 34.12-2018, введен в действие в качестве стандарта Российской Федерации с 1 июня 2019 г.) использует неприводимый над $\mathbb{F}_2$ многочлен $x^8 + x^7 + x^6 + x + 1$. Американский стандарт AES (Advanced Encryption Standard) использует неприводимый над $\mathbb{F}_2$ многочлен $x^8 + x^4 + x^3 + x + 1$.

Поле вычетов по простому модулю p – это поле $\mathbb{F}_p$, элементами которого служат числа $0, 1, \ldots, p-1$ (*вычеты*, т.е. остатки от деления на p). Операции в $\mathbb{F}_p$ определяются так: сумма (произведение) вычетов a и b – это остаток от деления на p обычной суммы (соответственно, обычного произведения) чисел a и b.

Неприводимые многочлены над полями вычетов имеют множество практических применений для передачи, хранения и защиты информации.

Например, шифр «Кузнечик» (стандарт ГОСТ 34.12-2018, введен в действие в качестве стандарта Российской Федерации с 1 июня 2019 г.) использует неприводимый над $\mathbb{F}_2$ многочлен $x^8 + x^7 + x^6 + x + 1$. Американский стандарт AES (Advanced Encryption Standard) использует неприводимый над $\mathbb{F}_2$ многочлен $x^8 + x^4 + x^3 + x + 1$.

В этой лекции обсудим неприводимые многочлены над $\mathbb{F}_p$.

Поле вычетов по простому модулю p – это поле $\mathbb{F}_p$, элементами которого служат числа $0, 1, \ldots, p-1$ (*вычеты*, т.е. остатки от деления на p). Операции в $\mathbb{F}_p$ определяются так: сумма (произведение) вычетов a и b – это остаток от деления на p обычной суммы (соответственно, обычного произведения) чисел a и b.

Неприводимые многочлены над полями вычетов имеют множество практических применений для передачи, хранения и защиты информации.

Например, шифр «Кузнечик» (стандарт ГОСТ 34.12-2018, введен в действие в качестве стандарта Российской Федерации с 1 июня 2019 г.) использует неприводимый над $\mathbb{F}_2$ многочлен $x^8 + x^7 + x^6 + x + 1$. Американский стандарт AES (Advanced Encryption Standard) использует неприводимый над $\mathbb{F}_2$ многочлен $x^8 + x^4 + x^3 + x + 1$.

В этой лекции обсудим неприводимые многочлены над $\mathbb{F}_p$. Самый первый вопрос таков. Всякий неприводимый над $\mathbb{C}$ многочлен линеен, а всякий неприводимый над $\mathbb{R}$ многочлен имеет степень $\leqslant 2$.

Поле вычетов по простому модулю p – это поле $\mathbb{F}_p$, элементами которого служат числа $0, 1, \ldots, p-1$ (*вычеты*, т.е. остатки от деления на p). Операции в $\mathbb{F}_p$ определяются так: сумма (произведение) вычетов a и b – это остаток от деления на p обычной суммы (соответственно, обычного произведения) чисел a и b.

Неприводимые многочлены над полями вычетов имеют множество практических применений для передачи, хранения и защиты информации.

Например, шифр «Кузнечик» (стандарт ГОСТ 34.12-2018, введен в действие в качестве стандарта Российской Федерации с 1 июня 2019 г.) использует неприводимый над $\mathbb{F}_2$ многочлен $x^8 + x^7 + x^6 + x + 1$. Американский стандарт AES (Advanced Encryption Standard) использует неприводимый над $\mathbb{F}_2$ многочлен $x^8 + x^4 + x^3 + x + 1$.

В этой лекции обсудим неприводимые многочлены над $\mathbb{F}_p$. Самый первый вопрос таков. Всякий неприводимый над $\mathbb{C}$ многочлен линеен, а всякий неприводимый над $\mathbb{R}$ многочлен имеет степень $\leqslant 2$. А степень неприводимого над $\mathbb{Q}$ многочлена может быть любой.

Поле вычетов по простому модулю p – это поле $\mathbb{F}_p$, элементами которого служат числа $0, 1, \ldots, p-1$ (*вычеты*, т.е. остатки от деления на p). Операции в $\mathbb{F}_p$ определяются так: сумма (произведение) вычетов a и b – это остаток от деления на p обычной суммы (соответственно, обычного произведения) чисел a и b.

Неприводимые многочлены над полями вычетов имеют множество практических применений для передачи, хранения и защиты информации.

Например, шифр «Кузнечик» (стандарт ГОСТ 34.12-2018, введен в действие в качестве стандарта Российской Федерации с 1 июня 2019 г.) использует неприводимый над $\mathbb{F}_2$ многочлен $x^8 + x^7 + x^6 + x + 1$. Американский стандарт AES (Advanced Encryption Standard) использует неприводимый над $\mathbb{F}_2$ многочлен $x^8 + x^4 + x^3 + x + 1$.

В этой лекции обсудим неприводимые многочлены над $\mathbb{F}_p$.
Самый первый вопрос таков. Всякий неприводимый над $\mathbb{C}$ многочлен линеен, а всякий неприводимый над $\mathbb{R}$ многочлен имеет степень $\leqslant 2$.
А степень неприводимого над $\mathbb{Q}$ многочлена может быть любой.
Как обстоит дело со степенями неприводимых многочленов над $\mathbb{F}_p$*?*

Поле вычетов по простому модулю p – это поле $\mathbb{F}_p$, элементами которого служат числа $0, 1, \ldots, p-1$ (*вычеты*, т.е. остатки от деления на p). Операции в $\mathbb{F}_p$ определяются так: сумма (произведение) вычетов a и b – это остаток от деления на p обычной суммы (соответственно, обычного произведения) чисел a и b.

Неприводимые многочлены над полями вычетов имеют множество практических применений для передачи, хранения и защиты информации.

Например, шифр «Кузнечик» (стандарт ГОСТ 34.12-2018, введен в действие в качестве стандарта Российской Федерации с 1 июня 2019 г.) использует неприводимый над $\mathbb{F}_2$ многочлен $x^8 + x^7 + x^6 + x + 1$. Американский стандарт AES (Advanced Encryption Standard) использует неприводимый над $\mathbb{F}_2$ многочлен $x^8 + x^4 + x^3 + x + 1$.

В этой лекции обсудим неприводимые многочлены над $\mathbb{F}_p$.
Самый первый вопрос таков. Всякий неприводимый над $\mathbb{C}$ многочлен линеен, а всякий неприводимый над $\mathbb{R}$ многочлен имеет степень $\leqslant 2$.
А степень неприводимого над $\mathbb{Q}$ многочлена может быть любой.
Как обстоит дело со степенями неприводимых многочленов над $\mathbb{F}_p$*?*
Докажем, что для любого простого числа p над полем вычетов $\mathbb{F}_p$ существуют неприводимые многочлены любой степени.

Идея

Начнем с простых соображений. Пусть $p = 2$. Над $\mathbb{F}_2$ есть 2 многочлена 1-й степени, 4 многочлена 2-й степени, 8 многочленов 3-й степени, ..., 2^n многочленов n-й степени.

Идея

Начнем с простых соображений. Пусть $p = 2$. Над $\mathbb{F}_2$ есть 2 многочлена 1-й степени, 4 многочлена 2-й степени, 8 многочленов 3-й степени, ..., 2^n многочленов n-й степени.

Многочлены 1-й степени неприводимы. Приводимые многочлены 2-й степени должны быть произведениями неприводимых, но из двух многочленов 1-й степени можно составить только три произведения 2-й степени.

Идея

Начнем с простых соображений. Пусть $p = 2$. Над $\mathbb{F}_2$ есть 2 многочлена 1-й степени, 4 многочлена 2-й степени, 8 многочленов 3-й степени, ..., 2^n многочленов n-й степени.

Многочлены 1-й степени неприводимы. Приводимые многочлены 2-й степени должны быть произведениями неприводимых, но из двух многочленов 1-й степени можно составить только три произведения 2-й степени. Поэтому из четырех многочленов 2-й степени один должен быть неприводим!

Начнем с простых соображений. Пусть $p = 2$. Над $\mathbb{F}_2$ есть 2 многочлена 1-й степени, 4 многочлена 2-й степени, 8 многочленов 3-й степени, ..., 2^n многочленов n-й степени.

Многочлены 1-й степени неприводимы. Приводимые многочлены 2-й степени должны быть произведениями неприводимых, но из двух многочленов 1-й степени можно составить только три произведения 2-й степени. Поэтому из четырех многочленов 2-й степени один должен быть неприводим!

Приводимые многочлены 3-й степени должны быть произведениями неприводимых 1-й и/или 2-й степени. Из двух многочленов 1-й степени и одного многочлена 2-й степени можно составить только шесть произведений 3-й степени.

Идея

Начнем с простых соображений. Пусть $p = 2$. Над $\mathbb{F}_2$ есть 2 многочлена 1-й степени, 4 многочлена 2-й степени, 8 многочленов 3-й степени, $\dots$, 2^n многочленов n-й степени.

Многочлены 1-й степени неприводимы. Приводимые многочлены 2-й степени должны быть произведениями неприводимых, но из двух многочленов 1-й степени можно составить только три произведения 2-й степени. Поэтому из четырех многочленов 2-й степени один должен быть неприводим!

Приводимые многочлены 3-й степени должны быть произведениями неприводимых 1-й и/или 2-й степени. Из двух многочленов 1-й степени и одного многочлена 2-й степени можно составить только шесть произведений 3-й степени. Поэтому из восьми многочленов 3-й степени два должны быть неприводимыми!

Начнем с простых соображений. Пусть $p = 2$. Над $\mathbb{F}_2$ есть 2 многочлена 1-й степени, 4 многочлена 2-й степени, 8 многочленов 3-й степени, ..., 2^n многочленов n-й степени.

Многочлены 1-й степени неприводимы. Приводимые многочлены 2-й степени должны быть произведениями неприводимых, но из двух многочленов 1-й степени можно составить только три произведения 2-й степени. Поэтому из четырех многочленов 2-й степени один должен быть неприводим!

Приводимые многочлены 3-й степени должны быть произведениями неприводимых 1-й и/или 2-й степени. Из двух многочленов 1-й степени и одного многочлена 2-й степени можно составить только шесть произведений 3-й степени. Поэтому из восьми многочленов 3-й степени два должны быть неприводимыми!

Возникает такая идея: доказать существование неприводимых многочленов n-й степени, подсчитав, что произведений неприводимых многочленов меньших степеней не хватит, чтобы получить все 2^n многочленов n-й степени.

Идея

Начнем с простых соображений. Пусть $p = 2$. Над $\mathbb{F}_2$ есть 2 многочлена 1-й степени, 4 многочлена 2-й степени, 8 многочленов 3-й степени, ..., 2^n многочленов n-й степени.

Многочлены 1-й степени неприводимы. Приводимые многочлены 2-й степени должны быть произведениями неприводимых, но из двух многочленов 1-й степени можно составить только три произведения 2-й степени. Поэтому из четырех многочленов 2-й степени один должен быть неприводим!

Приводимые многочлены 3-й степени должны быть произведениями неприводимых 1-й и/или 2-й степени. Из двух многочленов 1-й степени и одного многочлена 2-й степени можно составить только шесть произведений 3-й степени. Поэтому из восьми многочленов 3-й степени два должны быть неприводимыми!

Возникает такая идея: доказать существование неприводимых многочленов n-й степени, подсчитав, что произведений неприводимых многочленов меньших степеней не хватит, чтобы получить все 2^n многочленов n-й степени.

Чтобы реализовать эту идею (сразу для всех полей вычетов $\mathbb{F}_p$), удобно воспользоваться одним классическим приемом комбинаторики.

Пусть f – унитарный неприводимый многочлен степени m над полем $\mathbb{F}_p$.

Пусть f – унитарный неприводимый многочлен степени m над полем $\mathbb{F}_p$. Обозначим через A_k число многочленов степени k вида f^α, $\alpha = 0, 1, 2, \dots$.

Ясно, что $A_k = \begin{cases} 1, & \text{если} \quad m|k, \\ 0, & \text{если} \quad m \nmid k. \end{cases}$

Пусть f – унитарный неприводимый многочлен степени m над полем $\mathbb{F}_p$. Обозначим через A_k число многочленов степени k вида f^α, $\alpha = 0, 1, 2, \dots$.

Ясно, что $A_k = \begin{cases} 1, & \text{если} \quad m|k, \\ 0, & \text{если} \quad m \nmid k. \end{cases}$ Рассмотрим формальный ряд

$$A(z) := \sum_{k=0}^{\infty} A_k z^k = 1 + z^m + z^{2m} + \dots = \frac{1}{1 - z^m}.$$

Пусть f – унитарный неприводимый многочлен степени m над полем $\mathbb{F}_p$. Обозначим через A_k число многочленов степени k вида f^α, $\alpha = 0, 1, 2, \dots$.

Ясно, что $A_k = \begin{cases} 1, & \text{если } \ m|k, \\ 0, & \text{если } \ m \nmid k. \end{cases}$ Рассмотрим формальный ряд

$$A(z) := \sum_{k=0}^{\infty} A_k z^k = 1 + z^m + z^{2m} + \dots = \frac{1}{1 - z^m}.$$

Он называется *нумератором* множества $\{f^\alpha\}$.

Нумераторы

Пусть f – унитарный неприводимый многочлен степени m над полем $\mathbb{F}_p$. Обозначим через A_k число многочленов степени k вида f^α, $\alpha = 0, 1, 2, \ldots$.

Ясно, что $A_k = \begin{cases} 1, & \text{если} \quad m|k, \\ 0, & \text{если} \quad m \nmid k. \end{cases}$ Рассмотрим формальный ряд

$$A(z) := \sum_{k=0}^{\infty} A_k z^k = 1 + z^m + z^{2m} + \cdots = \frac{1}{1 - z^m}.$$

Он называется *нумератором* множества $\{f^\alpha\}$.

Пусть $B(z) := \sum_{k=0}^{\infty} B_k z^k$ – нумератор множества $\{g^\beta\}$, где g – другой унитарный неприводимый многочлен над $\mathbb{F}_p$.

Пусть f – унитарный неприводимый многочлен степени m над полем $\mathbb{F}_p$. Обозначим через A_k число многочленов степени k вида f^α, $\alpha = 0, 1, 2, \dots$.

Ясно, что $A_k = \begin{cases} 1, & \text{если} \quad m|k, \\ 0, & \text{если} \quad m \nmid k. \end{cases}$ Рассмотрим формальный ряд

$$A(z) := \sum_{k=0}^{\infty} A_k z^k = 1 + z^m + z^{2m} + \cdots = \frac{1}{1 - z^m}.$$

Он называется *нумератором* множества $\{f^\alpha\}$.

Пусть $B(z) := \sum_{k=0}^{\infty} B_k z^k$ – нумератор множества $\{g^\beta\}$, где g – другой унитарный неприводимый многочлен над $\mathbb{F}_p$. Рассмотрим множество $C := \{f^\alpha g^\beta\}$ и обозначим через C_k число многочленов степени k в C.

Пусть f – унитарный неприводимый многочлен степени m над полем $\mathbb{F}_p$. Обозначим через A_k число многочленов степени k вида f^α, $\alpha = 0, 1, 2, \dots$.
Ясно, что $A_k = \begin{cases} 1, & \text{если} \quad m|k, \\ 0, & \text{если} \quad m \nmid k. \end{cases}$ Рассмотрим формальный ряд

$$A(z) := \sum_{k=0}^{\infty} A_k z^k = 1 + z^m + z^{2m} + \dots = \frac{1}{1 - z^m}.$$

Он называется *нумератором* множества $\{f^\alpha\}$.

Пусть $B(z) := \sum_{k=0}^{\infty} B_k z^k$ – нумератор множества $\{g^\beta\}$, где g – другой унитарный неприводимый многочлен над $\mathbb{F}_p$. Рассмотрим множество $C := \{f^\alpha g^\beta\}$ и обозначим через C_k число многочленов степени k в C.
Ясно, что если $\deg f^\alpha g^\beta = k$, а $\deg f^\alpha = i$, то $\deg g^\beta = k - i$.

Пусть f – унитарный неприводимый многочлен степени m над полем $\mathbb{F}_p$. Обозначим через A_k число многочленов степени k вида f^α, $\alpha = 0, 1, 2, \ldots$.

Ясно, что $A_k = \begin{cases} 1, & \text{если} \quad m|k, \\ 0, & \text{если} \quad m \nmid k. \end{cases}$ Рассмотрим формальный ряд

$$A(z) := \sum_{k=0}^{\infty} A_k z^k = 1 + z^m + z^{2m} + \cdots = \frac{1}{1 - z^m}.$$

Он называется *нумератором* множества $\{f^\alpha\}$.

Пусть $B(z) := \sum_{k=0}^{\infty} B_k z^k$ – нумератор множества $\{g^\beta\}$, где g – другой унитарный неприводимый многочлен над $\mathbb{F}_p$. Рассмотрим множество $C := \{f^\alpha g^\beta\}$ и обозначим через C_k число многочленов степени k в C. Ясно, что если $\deg f^\alpha g^\beta = k$, а $\deg f^\alpha = i$, то $\deg g^\beta = k - i$. Поэтому $C_k = \sum_i A_i B_{k-i}$, откуда $C(z) := \sum_{k=0}^{\infty} C_k z^k = A(z)B(z)$.

Пусть f – унитарный неприводимый многочлен степени m над полем $\mathbb{F}_p$. Обозначим через A_k число многочленов степени k вида f^α, $\alpha = 0, 1, 2, \dots$. Ясно, что $A_k = \begin{cases} 1, & \text{если } m|k, \\ 0, & \text{если } m \nmid k. \end{cases}$ Рассмотрим формальный ряд

$$A(z) := \sum_{k=0}^{\infty} A_k z^k = 1 + z^m + z^{2m} + \dots = \frac{1}{1 - z^m}.$$

Он называется *нумератором* множества $\{f^\alpha\}$.

Пусть $B(z) := \sum_{k=0}^{\infty} B_k z^k$ – нумератор множества $\{g^\beta\}$, где g – другой унитарный неприводимый многочлен над $\mathbb{F}_p$. Рассмотрим множество $C := \{f^\alpha g^\beta\}$ и обозначим через C_k число многочленов степени k в C. Ясно, что если $\deg f^\alpha g^\beta = k$, а $\deg f^\alpha = i$, то $\deg g^\beta = k - i$. Поэтому $C_k = \sum_i A_i B_{k-i}$, откуда $C(z) := \sum_{k=0}^{\infty} C_k z^k = A(z)B(z)$.

Примеры: нумератор множества всех многочленов над $\mathbb{F}_2$, разлагающихся на линейные множители, равен $\dfrac{1}{(1-z)^2}$

Пусть f – унитарный неприводимый многочлен степени m над полем $\mathbb{F}_p$. Обозначим через A_k число многочленов степени k вида f^α, $\alpha = 0, 1, 2, \dots$.
Ясно, что $A_k = \begin{cases} 1, & \text{если } m|k, \\ 0, & \text{если } m \nmid k. \end{cases}$ Рассмотрим формальный ряд

$$A(z) := \sum_{k=0}^{\infty} A_k z^k = 1 + z^m + z^{2m} + \cdots = \frac{1}{1 - z^m}.$$

Он называется *нумератором* множества $\{f^\alpha\}$.

Пусть $B(z) := \sum_{k=0}^{\infty} B_k z^k$ – нумератор множества $\{g^\beta\}$, где g – другой унитарный неприводимый многочлен над $\mathbb{F}_p$. Рассмотрим множество $C := \{f^\alpha g^\beta\}$ и обозначим через C_k число многочленов степени k в C. Ясно, что если $\deg f^\alpha g^\beta = k$, а $\deg f^\alpha = i$, то $\deg g^\beta = k - i$. Поэтому $C_k = \sum_i A_i B_{k-i}$, откуда $C(z) := \sum_{k=0}^{\infty} C_k z^k = A(z)B(z)$.

Примеры: нумератор множества всех многочленов над $\mathbb{F}_2$, разлагающихся на линейные множители, равен $\dfrac{1}{(1-z)^2}$; нумератор множества всех многочленов над $\mathbb{F}_2$, разлагающихся на неприводимые множители степени $\leqslant 2$, равен $\dfrac{1}{(1-z)^2} \cdot \dfrac{1}{1-z^2}$.

Число неприводимых многочленов данной степени над $\mathbb{F}_p$

Если I_m – число унитарных неприводимых многочленов степени m над $\mathbb{F}_p$, то

$$P(z) := \prod_{m=1}^{\infty} \frac{1}{(1-z^m)^{I_m}}$$

есть нумератор множества всех многочленов над $\mathbb{F}_p$, разлагающихся на унитарные неприводимые множители.

Число неприводимых многочленов данной степени над $\mathbb{F}_p$

Если I_m – число унитарных неприводимых многочленов степени m над $\mathbb{F}_p$, то

$$P(z) := \prod_{m=1}^{\infty} \frac{1}{(1-z^m)^{I_m}}$$

есть нумератор множества всех многочленов над $\mathbb{F}_p$, разлагающихся на унитарные неприводимые множители. Но по теореме о разложении многочлена на неприводимые множители, каждый унитарный многочлен над $\mathbb{F}_p$ однозначно разлагается на унитарные неприводимые множители!

Если I_m – число унитарных неприводимых многочленов степени m над $\mathbb{F}_p$, то

$$P(z) := \prod_{m=1}^{\infty} \frac{1}{(1 - z^m)^{I_m}}$$

есть нумератор множества всех многочленов над $\mathbb{F}_p$, разлагающихся на унитарные неприводимые множители. Но по теореме о разложении многочлена на неприводимые множители, каждый унитарный многочлен над $\mathbb{F}_p$ однозначно разлагается на унитарные неприводимые множители! Поэтому $P(z)$ – нумератор множества всех унитарных многочленов

Если I_m – число унитарных неприводимых многочленов степени m над $\mathbb{F}_p$, то

$$P(z) := \prod_{m=1}^{\infty} \frac{1}{(1-z^m)^{I_m}}$$

есть нумератор множества всех многочленов над $\mathbb{F}_p$, разлагающихся на унитарные неприводимые множители. Но по теореме о разложении многочлена на неприводимые множители, каждый унитарный многочлен над $\mathbb{F}_p$ однозначно разлагается на унитарные неприводимые множители! Поэтому $P(z)$ – нумератор множества всех унитарных многочленов, т.е.

$$P(z) = 1 + pz + p^2z^2 + \cdots + p^kz^k + \cdots = \frac{1}{1-pz}.$$

Если I_m – число унитарных неприводимых многочленов степени m над $\mathbb{F}_p$, то

$$P(z) := \prod_{m=1}^{\infty} \frac{1}{(1-z^m)^{I_m}}$$

есть нумератор множества всех многочленов над $\mathbb{F}_p$, разлагающихся на унитарные неприводимые множители. Но по теореме о разложении многочлена на неприводимые множители, каждый унитарный многочлен над $\mathbb{F}_p$ однозначно разлагается на унитарные неприводимые множители! Поэтому $P(z)$ – нумератор множества всех унитарных многочленов, т.е.

$$P(z) = 1 + pz + p^2z^2 + \cdots + p^kz^k + \cdots = \frac{1}{1-pz}.$$

Итак,

$$\frac{1}{1-pz} = \prod_{m=1}^{\infty} \frac{1}{(1-z^m)^{I_m}}.$$

Если I_m – число унитарных неприводимых многочленов степени m над $\mathbb{F}_p$, то

$$P(z) := \prod_{m=1}^{\infty} \frac{1}{(1-z^m)^{I_m}}$$

есть нумератор множества всех многочленов над $\mathbb{F}_p$, разлагающихся на унитарные неприводимые множители. Но по теореме о разложении многочлена на неприводимые множители, каждый унитарный многочлен над $\mathbb{F}_p$ однозначно разлагается на унитарные неприводимые множители! Поэтому $P(z)$ – нумератор множества всех унитарных многочленов, т.е.

$$P(z) = 1 + pz + p^2z^2 + \cdots + p^kz^k + \cdots = \frac{1}{1-pz}.$$

Итак,

$$\frac{1}{1-pz} = \prod_{m=1}^{\infty} \frac{1}{(1-z^m)^{I_m}}.$$

Отсюда,

$$1 - pz = \prod_{m=1}^{\infty} (1-z^m)^{I_m}.$$

Число неприводимых многочленов данной степени над $\mathbb{F}_p$ (2)

$$1 - pz = \prod_{m=1}^{\infty} (1 - z^m)^{I_m}.$$

$$1 - pz = \prod_{m=1}^{\infty} (1 - z^m)^{I_m}.$$

$$1 - pz = \prod_{m=1}^{\infty} (1 - z^m)^{I_m}.$$

Возьмем логарифмическую производную обеих частей $\left((\ln y)' = \dfrac{y'}{y}\right)$.

$$1 - pz = \prod_{m=1}^{\infty} (1 - z^m)^{I_m}.$$

Возьмем логарифмическую производную обеих частей $\left((\ln y)' = \dfrac{y'}{y}\right)$.

$$\frac{-p}{1-pz} = \sum_{m=1}^{\infty} \frac{-mI_m z^{m-1}}{1-z^m}.$$

$$1 - pz = \prod_{m=1}^{\infty} (1 - z^m)^{I_m}.$$

Возьмем логарифмическую производную обеих частей $\left((\ln y)' = \dfrac{y'}{y}\right)$.

$$\frac{-p}{1 - pz} = \sum_{m=1}^{\infty} \frac{-mI_m z^{m-1}}{1 - z^m}.$$

Умножим обе части на $-z$:

$$\frac{pz}{1 - pz} = \sum_{m=1}^{\infty} mI_m \frac{z^m}{1 - z^m}.$$

$$1 - pz = \prod_{m=1}^{\infty} (1 - z^m)^{I_m}.$$

Возьмем логарифмическую производную обеих частей $\left((\ln y)' = \dfrac{y'}{y}\right)$.

$$\frac{-p}{1 - pz} = \sum_{m=1}^{\infty} \frac{-mI_m z^{m-1}}{1 - z^m}.$$

Умножим обе части на $-z$:

$$\frac{pz}{1 - pz} = \sum_{m=1}^{\infty} mI_m \frac{z^m}{1 - z^m}.$$

Развернув суммы прогрессий в обеих частях, получим

$$\sum_{k=1}^{\infty} p^k z^k = \sum_{m=1}^{\infty} mI_m \sum_{m|k} z^k = \sum_{k=1} \left(\sum_{m|k} mI_m \right) z^k.$$

$$1 - pz = \prod_{m=1}^{\infty} (1 - z^m)^{I_m}.$$

Возьмем логарифмическую производную обеих частей $\left((\ln y)' = \dfrac{y'}{y} \right)$.

$$\frac{-p}{1-pz} = \sum_{m=1}^{\infty} \frac{-mI_m z^{m-1}}{1-z^m}.$$

Умножим обе части на $-z$:

$$\frac{pz}{1-pz} = \sum_{m=1}^{\infty} mI_m \frac{z^m}{1-z^m}.$$

Развернув суммы прогрессий в обеих частях, получим

$$\sum_{k=1}^{\infty} p^k z^k = \sum_{m=1}^{\infty} mI_m \sum_{m|k} z^k = \sum_{k=1} \left(\sum_{m|k} mI_m \right) z^k.$$

Приравняв коэффициенты при z^k, получим

$$\sum_{m|k} mI_m = p^k.$$

$$\boxed{\sum_{m|k} mI_m = p^k}$$

$$\boxed{\sum_{m|k} mI_m = p^k}$$

Отсюда $I_1 = p$ (что, впрочем, и так ясно).

$$\boxed{\sum_{m|k} mI_m = p^k}$$

Отсюда $I_1 = p$ (что, впрочем, и так ясно).

При $k = 2$ имеем $I_1 + 2I_2 = p^2$, откуда $I_2 = \dfrac{p^2 - p}{2} > 0$.

$$\boxed{\sum_{m|k} mI_m = p^k}$$

Отсюда $I_1 = p$ (что, впрочем, и так ясно).

При $k = 2$ имеем $I_1 + 2I_2 = p^2$, откуда $I_2 = \dfrac{p^2 - p}{2} > 0$.

При $k = 3$ имеем $I_1 + 3I_3 = p^3$, откуда $I_3 = \dfrac{p^3 - p}{3} > 0$.

$$\boxed{\sum_{m|k} mI_m = p^k}$$

Отсюда $I_1 = p$ (что, впрочем, и так ясно).

При $k = 2$ имеем $I_1 + 2I_2 = p^2$, откуда $I_2 = \dfrac{p^2 - p}{2} > 0$.

При $k = 3$ имеем $I_1 + 3I_3 = p^3$, откуда $I_3 = \dfrac{p^3 - p}{3} > 0$.

Вообще, при простом k имеем $I_1 + kI_k = p^k$, откуда $I_k = \dfrac{p^k - p}{k}$.

$$\boxed{\sum_{m|k} mI_m = p^k}$$

Отсюда $I_1 = p$ (что, впрочем, и так ясно).

При $k = 2$ имеем $I_1 + 2I_2 = p^2$, откуда $I_2 = \dfrac{p^2 - p}{2} > 0$.

При $k = 3$ имеем $I_1 + 3I_3 = p^3$, откуда $I_3 = \dfrac{p^3 - p}{3} > 0$.

Вообще, при простом k имеем $I_1 + kI_k = p^k$, откуда $I_k = \dfrac{p^k - p}{k}$.

При любом k имеем $I_k \leq \dfrac{p^k - p}{k}$.

$$\boxed{\sum_{m|k} mI_m = p^k}$$

Отсюда $I_1 = p$ (что, впрочем, и так ясно).

При $k = 2$ имеем $I_1 + 2I_2 = p^2$, откуда $I_2 = \dfrac{p^2 - p}{2} > 0$.

При $k = 3$ имеем $I_1 + 3I_3 = p^3$, откуда $I_3 = \dfrac{p^3 - p}{3} > 0$.

Вообще, при простом k имеем $I_1 + kI_k = p^k$, откуда $I_k = \dfrac{p^k - p}{k}$.

При любом k имеем $I_k \leq \dfrac{p^k - p}{k}$. С другой стороны,

$$p^k = \sum_{m|k} mI_m$$

$$\boxed{\sum_{m|k} mI_m = p^k}$$

Отсюда $I_1 = p$ (что, впрочем, и так ясно).

При $k = 2$ имеем $I_1 + 2I_2 = p^2$, откуда $I_2 = \dfrac{p^2 - p}{2} > 0$.

При $k = 3$ имеем $I_1 + 3I_3 = p^3$, откуда $I_3 = \dfrac{p^3 - p}{3} > 0$.

Вообще, при простом k имеем $I_1 + kI_k = p^k$, откуда $I_k = \dfrac{p^k - p}{k}$.

При любом k имеем $I_k \leq \dfrac{p^k - p}{k}$. С другой стороны,

$$p^k = \sum_{m|k} mI_m = kI_k + \sum_{m|k,\, m \leq \frac{k}{2}} mI_m$$

$$\boxed{\sum_{m|k} mI_m = p^k}$$

Отсюда $I_1 = p$ (что, впрочем, и так ясно).

При $k = 2$ имеем $I_1 + 2I_2 = p^2$, откуда $I_2 = \dfrac{p^2 - p}{2} > 0$.

При $k = 3$ имеем $I_1 + 3I_3 = p^3$, откуда $I_3 = \dfrac{p^3 - p}{3} > 0$.

Вообще, при простом k имеем $I_1 + kI_k = p^k$, откуда $I_k = \dfrac{p^k - p}{k}$.

При любом k имеем $I_k \leq \dfrac{p^k - p}{k}$. С другой стороны,

$$p^k = \sum_{m|k} mI_m = kI_k + \sum_{m|k,\, m \leq \frac{k}{2}} mI_m < kI_k + \sum_{j=1}^{\lfloor \frac{k}{2} \rfloor} p^j$$

$$\boxed{\sum_{m|k} mI_m = p^k}$$

Отсюда $I_1 = p$ (что, впрочем, и так ясно).

При $k = 2$ имеем $I_1 + 2I_2 = p^2$, откуда $I_2 = \dfrac{p^2 - p}{2} > 0$.

При $k = 3$ имеем $I_1 + 3I_3 = p^3$, откуда $I_3 = \dfrac{p^3 - p}{3} > 0$.

Вообще, при простом k имеем $I_1 + kI_k = p^k$, откуда $I_k = \dfrac{p^k - p}{k}$.

При любом k имеем $I_k \le \dfrac{p^k - p}{k}$. С другой стороны,

$$p^k = \sum_{m|k} mI_m = kI_k + \sum_{m|k,\, m\le\frac{k}{2}} mI_m < kI_k + \sum_{j=1}^{\lfloor\frac{k}{2}\rfloor} p^j < kI_k + p^{\lfloor\frac{k}{2}\rfloor+1}.$$

$$\boxed{\sum_{m|k} mI_m = p^k}$$

Отсюда $I_1 = p$ (что, впрочем, и так ясно).

При $k = 2$ имеем $I_1 + 2I_2 = p^2$, откуда $I_2 = \dfrac{p^2 - p}{2} > 0$.

При $k = 3$ имеем $I_1 + 3I_3 = p^3$, откуда $I_3 = \dfrac{p^3 - p}{3} > 0$.

Вообще, при простом k имеем $I_1 + kI_k = p^k$, откуда $I_k = \dfrac{p^k - p}{k}$.

При любом k имеем $I_k \leq \dfrac{p^k - p}{k}$. С другой стороны,

$$p^k = \sum_{m|k} mI_m = kI_k + \sum_{m|k,\, m \leq \frac{k}{2}} mI_m < kI_k + \sum_{j=1}^{\lfloor \frac{k}{2} \rfloor} p^j < kI_k + p^{\lfloor \frac{k}{2} \rfloor + 1}.$$

Отсюда $I_k > \dfrac{p^k - p^{\lfloor \frac{k}{2} \rfloor + 1}}{k} = \dfrac{p^k}{k}\left(1 - p^{-\lceil \frac{k}{2} \rceil + 1}\right) \geq 0.$

$$\boxed{\sum_{m|k} mI_m = p^k}$$

Отсюда $I_1 = p$ (что, впрочем, и так ясно).

При $k = 2$ имеем $I_1 + 2I_2 = p^2$, откуда $I_2 = \dfrac{p^2 - p}{2} > 0$.

При $k = 3$ имеем $I_1 + 3I_3 = p^3$, откуда $I_3 = \dfrac{p^3 - p}{3} > 0$.

Вообще, при простом k имеем $I_1 + kI_k = p^k$, откуда $I_k = \dfrac{p^k - p}{k}$.

При любом k имеем $I_k \leq \dfrac{p^k - p}{k}$. С другой стороны,

$$p^k = \sum_{m|k} mI_m = kI_k + \sum_{m|k,\, m\leq\frac{k}{2}} mI_m < kI_k + \sum_{j=1}^{\lfloor\frac{k}{2}\rfloor} p^j < kI_k + p^{\lfloor\frac{k}{2}\rfloor+1}.$$

Отсюда $I_k > \dfrac{p^k - p^{\lfloor\frac{k}{2}\rfloor+1}}{k} = \dfrac{p^k}{k}\left(1 - p^{-\lceil\frac{k}{2}\rceil+1}\right) \geq 0$. Итак, $I_k > 0$.

Доказав, что $I_k > 0$ при всех k, мы доказали, что для любого простого числа p над полем вычетов $\mathbb{F}_p$ существуют неприводимые многочлены любой степени.

Формула обращения Мёбиуса

Доказав, что $I_k > 0$ при всех k, мы доказали, что для любого простого числа p над полем вычетов $\mathbb{F}_p$ существуют неприводимые многочлены любой степени. Нетрудно получить и явную формулу для числа I_k.

Доказав, что $I_k > 0$ при всех k, мы доказали, что для любого простого числа p над полем вычетов $\mathbb{F}_p$ существуют неприводимые многочлены любой степени. Нетрудно получить и явную формулу для числа I_k.
Функция Мёбиуса $\mu\colon \mathbb{N} \to \{-1, 0, 1\}$ определяется так:

$$\mu(d) := \begin{cases} 1, & \text{если } \ d = 1, \\ (-1)^k, & \text{если } d \text{ – произведение } k \text{ различных простых чисел}, \\ 0, & \text{если } d \text{ делится на квадрат простого числа}. \end{cases}$$

Доказав, что $I_k > 0$ при всех k, мы доказали, что для любого простого числа p над полем вычетов $\mathbb{F}_p$ существуют неприводимые многочлены любой степени. Нетрудно получить и явную формулу для числа I_k.
Функция Мёбиуса $\mu\colon \mathbb{N} \to \{-1, 0, 1\}$ определяется так:

$$\mu(d) := \begin{cases} 1, & \text{если} \quad d = 1, \\ (-1)^k, & \text{если } d \text{ – произведение } k \text{ различных простых чисел,} \\ 0, & \text{если } d \text{ делится на квадрат простого числа.} \end{cases}$$

Нам понадобится такое свойство функции Мёбиуса:

$$\sum_{d|n} \mu(d) = \begin{cases} 1, & \text{если} \quad n = 1, \\ 0, & \text{если} \quad n > 1. \end{cases}$$

Доказав, что $I_k > 0$ при всех k, мы доказали, что для любого простого числа p над полем вычетов $\mathbb{F}_p$ существуют неприводимые многочлены любой степени. Нетрудно получить и явную формулу для числа I_k.
Функция Мёбиуса $\mu\colon \mathbb{N} \to \{-1, 0, 1\}$ определяется так:

$$\mu(d) := \begin{cases} 1, & \text{если } \ d = 1, \\ (-1)^k, & \text{если } d \text{ – произведение } k \text{ различных простых чисел,} \\ 0, & \text{если } d \text{ делится на квадрат простого числа.} \end{cases}$$

Нам понадобится такое свойство функции Мёбиуса:

$$\sum_{d|n} \mu(d) = \begin{cases} 1, & \text{если } \ n = 1, \\ 0, & \text{если } \ n > 1. \end{cases}$$

Доказательство. Случай $n = 1$ тривиален. Если $n > 1$, то пусть $p_1, \ldots, p_k$ – все различные простые делители числа n.

Доказав, что $I_k > 0$ при всех k, мы доказали, что для любого простого числа p над полем вычетов $\mathbb{F}_p$ существуют неприводимые многочлены любой степени. Нетрудно получить и явную формулу для числа I_k. *Функция Мёбиуса* $\mu\colon \mathbb{N} \to \{-1, 0, 1\}$ определяется так:

$$\mu(d) := \begin{cases} 1, & \text{если } d = 1, \\ (-1)^k, & \text{если } d \text{ -- произведение } k \text{ различных простых чисел,} \\ 0, & \text{если } d \text{ делится на квадрат простого числа.} \end{cases}$$

Нам понадобится такое свойство функции Мёбиуса:

$$\sum_{d|n} \mu(d) = \begin{cases} 1, & \text{если } n = 1, \\ 0, & \text{если } n > 1. \end{cases}$$

Доказательство. Случай $n = 1$ тривиален. Если $n > 1$, то пусть $p_1, \dots, p_k$ – все различные простые делители числа n. Отличные от нуля слагаемые суммы $\sum_{d|n} \mu(d)$ отвечают подмножествам множества $\{p_1, \dots, p_k\}$.

Доказав, что $I_k > 0$ при всех k, мы доказали, что для любого простого числа p над полем вычетов $\mathbb{F}_p$ существуют неприводимые многочлены любой степени. Нетрудно получить и явную формулу для числа I_k.
Функция Мёбиуса $\mu\colon \mathbb{N} \to \{-1, 0, 1\}$ определяется так:

$$\mu(d) := \begin{cases} 1, & \text{если } \ d = 1, \\ (-1)^k, & \text{если } d \text{ – произведение } k \text{ различных простых чисел,} \\ 0, & \text{если } d \text{ делится на квадрат простого числа.} \end{cases}$$

Нам понадобится такое свойство функции Мёбиуса:

$$\sum_{d|n} \mu(d) = \begin{cases} 1, & \text{если } \ n = 1, \\ 0, & \text{если } \ n > 1. \end{cases}$$

Доказательство. Случай $n = 1$ тривиален. Если $n > 1$, то пусть $p_1, \ldots, p_k$ – все различные простые делители числа n. Отличные от нуля слагаемые суммы $\sum_{d|n} \mu(d)$ отвечают подмножествам множества $\{p_1, \ldots, p_k\}$.
У любого непустого конечного множества подмножеств с четным и нечетным числом поровну (*объясните, почему!*).

Доказав, что $I_k > 0$ при всех k, мы доказали, что для любого простого числа p над полем вычетов $\mathbb{F}_p$ существуют неприводимые многочлены любой степени. Нетрудно получить и явную формулу для числа I_k.
Функция Мёбиуса $\mu\colon \mathbb{N} \to \{-1, 0, 1\}$ определяется так:

$$\mu(d) := \begin{cases} 1, & \text{если} \quad d = 1, \\ (-1)^k, & \text{если } d \text{ – произведение } k \text{ различных простых чисел,} \\ 0, & \text{если } d \text{ делится на квадрат простого числа.} \end{cases}$$

Нам понадобится такое свойство функции Мёбиуса:

$$\sum_{d|n} \mu(d) = \begin{cases} 1, & \text{если} \quad n = 1, \\ 0, & \text{если} \quad n > 1. \end{cases}$$

Доказательство. Случай $n = 1$ тривиален. Если $n > 1$, то пусть $p_1, \dots, p_k$ – все различные простые делители числа n. Отличные от нуля слагаемые суммы $\sum_{d|n} \mu(d)$ отвечают подмножествам множества $\{p_1, \dots, p_k\}$.
У любого непустого конечного множества подмножеств с четным и нечетным числом поровну (*объясните, почему!*). Поэтому слагаемых, равных 1, в сумме $\sum_{d|n} \mu(d)$ столько же, сколько слагаемых, равных -1

Доказав, что $I_k > 0$ при всех k, мы доказали, что для любого простого числа p над полем вычетов $\mathbb{F}_p$ существуют неприводимые многочлены любой степени. Нетрудно получить и явную формулу для числа I_k.

Функция Мёбиуса $\mu\colon \mathbb{N} \to \{-1, 0, 1\}$ определяется так:

$$\mu(d) := \begin{cases} 1, & \text{если} \quad d = 1, \\ (-1)^k, & \text{если } d \text{ – произведение } k \text{ различных простых чисел,} \\ 0, & \text{если } d \text{ делится на квадрат простого числа.} \end{cases}$$

Нам понадобится такое свойство функции Мёбиуса:

$$\sum_{d|n} \mu(d) = \begin{cases} 1, & \text{если} \quad n = 1, \\ 0, & \text{если} \quad n > 1. \end{cases}$$

Доказательство. Случай $n = 1$ тривиален. Если $n > 1$, то пусть $p_1, \ldots, p_k$ – все различные простые делители числа n. Отличные от нуля слагаемые суммы $\sum_{d|n} \mu(d)$ отвечают подмножествам множества $\{p_1, \ldots, p_k\}$.

У любого непустого конечного множества подмножеств с четным и нечетным числом поровну (*объясните, почему!*). Поэтому слагаемых, равных 1, в сумме $\sum_{d|n} \mu(d)$ столько же, сколько слагаемых, равных -1, а следовательно, сумма равна 0. $\square$

Теперь несложно доказать весьма полезную формулу:

Формула обращения Мёбиуса

Пусть функции $G\colon \mathbb{N} \to \mathbb{N}$ *и* $f\colon \mathbb{N} \to \mathbb{N}$ *таковы, что*

$$G(n) = \sum\nolimits_{d|n} f(d). \qquad (\star)$$

Тогда $f(n) = \sum_{d|n} \mu(d) G\left(\frac{n}{d}\right)$.

Теперь несложно доказать весьма полезную формулу:

Формула обращения Мёбиуса

Пусть функции $G\colon \mathbb{N} \to \mathbb{N}$ *и* $f\colon \mathbb{N} \to \mathbb{N}$ *таковы, что*

$$G(n) = \sum\nolimits_{d|n} f(d). \qquad (\star)$$

Тогда $f(n) = \sum_{d|n} \mu(d) G\left(\frac{n}{d}\right)$.

Доказательство. Подставим в $\sum_{d|n} \mu(d) G\left(\frac{n}{d}\right)$ выражение для G из $(\star)$:

$$\sum\nolimits_{d|n} \mu(d) G\left(\frac{n}{d}\right) = \sum\nolimits_{d|n} \mu(d) \sum\nolimits_{\delta|\frac{n}{d}} f(\delta).$$

Теперь несложно доказать весьма полезную формулу:

Формула обращения Мёбиуса

Пусть функции $G\colon \mathbb{N} \to \mathbb{N}$ *и* $f\colon \mathbb{N} \to \mathbb{N}$ *таковы, что*

$$G(n) = \sum\nolimits_{d|n} f(d). \qquad (\star)$$

Тогда $f(n) = \sum_{d|n} \mu(d) G\left(\frac{n}{d}\right)$.

Доказательство. Подставим в $\sum_{d|n} \mu(d) G\left(\frac{n}{d}\right)$ выражение для G из $(\star)$:

$$\sum\nolimits_{d|n} \mu(d) G\left(\frac{n}{d}\right) = \sum\nolimits_{d|n} \mu(d) \sum\nolimits_{\delta|\frac{n}{d}} f(\delta).$$

Ясно, что $\delta|\dfrac{n}{d}$, если и только если $\delta d|n$, если и только если $d|\dfrac{n}{\delta}$.

Теперь несложно доказать весьма полезную формулу:

Формула обращения Мёбиуса

Пусть функции $G\colon \mathbb{N}\to\mathbb{N}$ *и* $f\colon \mathbb{N}\to\mathbb{N}$ *таковы, что*

$$G(n)=\sum\nolimits_{d\mid n} f(d). \qquad (\star)$$

Тогда $f(n)=\sum_{d\mid n}\mu(d)G\left(\frac{n}{d}\right)$.

Доказательство. Подставим в $\sum_{d\mid n}\mu(d)G\left(\frac{n}{d}\right)$ выражение для G из $(\star)$:

$$\sum\nolimits_{d\mid n}\mu(d)G\left(\frac{n}{d}\right)=\sum\nolimits_{d\mid n}\mu(d)\sum\nolimits_{\delta\mid\frac{n}{d}} f(\delta).$$

Ясно, что $\delta\mid\dfrac{n}{d}$, если и только если $\delta d\mid n$, если и только если $d\mid\dfrac{n}{\delta}$. Поэтому

$$\sum\nolimits_{d\mid n}\mu(d)\sum\nolimits_{\delta\mid\frac{n}{d}} f(\delta)=\sum\nolimits_{\delta\mid n} f(\delta)\sum\nolimits_{d\mid\frac{n}{\delta}}\mu(d)=f(n),$$

поскольку $\sum_{d\mid\frac{n}{\delta}}\mu(d)=\begin{cases}1, & \text{если } \frac{n}{\delta}=1,\\ 0, & \text{если } \frac{n}{\delta}>1.\end{cases}$ $\square$

Напомним формулу, доказанную выше:

$$\sum_{d|n} dI_d = p^n.$$

Напомним формулу, доказанную выше:

$$\sum_{d|n} dI_d = p^n.$$

Она принимает вид $(\star)$, если положить $G(n) := p^n$, $f(d) := dI_d$.

Напомним формулу, доказанную выше:

$$\sum_{d|n} dI_d = p^n.$$

Она принимает вид $(\star)$, если положить $G(n) := p^n$, $f(d) := dI_d$. По формуле обращения Мёбиуса $f(n) = \sum_{d|n} \mu(d) G\left(\frac{n}{d}\right)$, т.е.

$$nI_n = \sum_{d|n} \mu(d) p^{\frac{n}{d}}.$$

Напомним формулу, доказанную выше:

$$\sum_{d|n} dI_d = p^n.$$

Она принимает вид $(\star)$, если положить $G(n) := p^n$, $f(d) := dI_d$. По формуле обращения Мёбиуса $f(n) = \sum_{d|n} \mu(d) G\left(\frac{n}{d}\right)$, т.е.

$$nI_n = \sum_{d|n} \mu(d) p^{\frac{n}{d}}.$$

Окончательно,

$$\boxed{I_n = \frac{1}{n} \sum_{d|n} \mu(d) p^{\frac{n}{d}}}$$

Напомним формулу, доказанную выше:

$$\sum_{d|n} dI_d = p^n.$$

Она принимает вид $(\star)$, если положить $G(n) := p^n$, $f(d) := dI_d$. По формуле обращения Мёбиуса $f(n) = \sum_{d|n} \mu(d)G\left(\frac{n}{d}\right)$, т.е.

$$nI_n = \sum_{d|n} \mu(d)p^{\frac{n}{d}}.$$

Окончательно,

$$\boxed{I_n = \frac{1}{n}\sum_{d|n} \mu(d)p^{\frac{n}{d}}}$$

Пример: число неприводимых многочленов 10-й степени над $\mathbb{F}_2$ равно $\frac{1}{10}\sum_{d|10} \mu(d)2^{\frac{10}{d}}$.

Напомним формулу, доказанную выше:

$$\sum_{d|n} dI_d = p^n.$$

Она принимает вид $(\star)$, если положить $G(n) := p^n$, $f(d) := dI_d$.
По формуле обращения Мёбиуса $f(n) = \sum_{d|n} \mu(d)G\left(\frac{n}{d}\right)$, т.е.

$$nI_n = \sum_{d|n} \mu(d)p^{\frac{n}{d}}.$$

Окончательно,

$$\boxed{I_n = \frac{1}{n}\sum_{d|n} \mu(d)p^{\frac{n}{d}}}$$

Пример: число неприводимых многочленов 10-й степени над $\mathbb{F}_2$ равно $\frac{1}{10}\sum_{d|10} \mu(d)2^{\frac{10}{d}}$. Делители 10 суть 1, 2, 5, 10; имеем $\mu(1) = \mu(10) = 1$, $\mu(2) = \mu(5) = -1$.

Напомним формулу, доказанную выше:

$$\sum_{d|n} dI_d = p^n.$$

Она принимает вид $(\star)$, если положить $G(n) := p^n$, $f(d) := dI_d$.
По формуле обращения Мёбиуса $f(n) = \sum_{d|n} \mu(d)G\left(\frac{n}{d}\right)$, т.е.

$$nI_n = \sum_{d|n} \mu(d)p^{\frac{n}{d}}.$$

Окончательно,

$$\boxed{I_n = \frac{1}{n}\sum_{d|n} \mu(d)p^{\frac{n}{d}}}$$

Пример: число неприводимых многочленов 10-й степени над $\mathbb{F}_2$ равно $\frac{1}{10}\sum_{d|10} \mu(d)2^{\frac{10}{d}}$. Делители 10 суть 1, 2, 5, 10; имеем $\mu(1) = \mu(10) = 1$, $\mu(2) = \mu(5) = -1$. Поэтому

$$\frac{1}{10}\sum_{d|10} \mu(d)2^{\frac{10}{d}}$$

Напомним формулу, доказанную выше:

$$\sum_{d|n} dI_d = p^n.$$

Она принимает вид $(\star)$, если положить $G(n) := p^n$, $f(d) := dI_d$.
По формуле обращения Мёбиуса $f(n) = \sum_{d|n} \mu(d) G\left(\frac{n}{d}\right)$, т.е.

$$nI_n = \sum_{d|n} \mu(d) p^{\frac{n}{d}}.$$

Окончательно,

$$\boxed{I_n = \frac{1}{n} \sum_{d|n} \mu(d) p^{\frac{n}{d}}}$$

Пример: число неприводимых многочленов 10-й степени над $\mathbb{F}_2$ равно $\frac{1}{10}\sum_{d|10} \mu(d) 2^{\frac{10}{d}}$. Делители 10 суть 1, 2, 5, 10; имеем $\mu(1) = \mu(10) = 1$, $\mu(2) = \mu(5) = -1$. Поэтому

$$\frac{1}{10} \sum_{d|10} \mu(d) 2^{\frac{10}{d}} = \frac{1}{10}\left(2^{10} - 2^5 - 2^2 + 2\right)$$

Напомним формулу, доказанную выше:

$$\sum_{d|n} dI_d = p^n.$$

Она принимает вид $(\star)$, если положить $G(n) := p^n$, $f(d) := dI_d$.
По формуле обращения Мёбиуса $f(n) = \sum_{d|n} \mu(d) G\left(\frac{n}{d}\right)$, т.е.

$$nI_n = \sum_{d|n} \mu(d) p^{\frac{n}{d}}.$$

Окончательно,

$$\boxed{I_n = \frac{1}{n} \sum_{d|n} \mu(d) p^{\frac{n}{d}}}$$

Пример: число неприводимых многочленов 10-й степени над $\mathbb{F}_2$ равно $\frac{1}{10} \sum_{d|10} \mu(d) 2^{\frac{10}{d}}$. Делители 10 суть 1, 2, 5, 10; имеем $\mu(1) = \mu(10) = 1$, $\mu(2) = \mu(5) = -1$. Поэтому

$$\frac{1}{10} \sum_{d|10} \mu(d) 2^{\frac{10}{d}} = \frac{1}{10} \left(2^{10} - 2^5 - 2^2 + 2\right) = \frac{1}{10} (1024 - 32 - 4 + 2)$$

Напомним формулу, доказанную выше:

$$\sum_{d|n} dI_d = p^n.$$

Она принимает вид $(\star)$, если положить $G(n) := p^n$, $f(d) := dI_d$.
По формуле обращения Мёбиуса $f(n) = \sum_{d|n} \mu(d) G\left(\frac{n}{d}\right)$, т.е.

$$nI_n = \sum_{d|n} \mu(d) p^{\frac{n}{d}}.$$

Окончательно,

$$\boxed{I_n = \frac{1}{n} \sum_{d|n} \mu(d) p^{\frac{n}{d}}}$$

Пример: число неприводимых многочленов 10-й степени над $\mathbb{F}_2$ равно $\frac{1}{10} \sum_{d|10} \mu(d) 2^{\frac{10}{d}}$. Делители 10 суть 1, 2, 5, 10; имеем $\mu(1) = \mu(10) = 1$, $\mu(2) = \mu(5) = -1$. Поэтому

$$\frac{1}{10} \sum_{d|10} \mu(d) 2^{\frac{10}{d}} = \frac{1}{10}\left(2^{10} - 2^5 - 2^2 + 2\right) = \frac{1}{10}(1024 - 32 - 4 + 2) = 99.$$

Для задачи *распознавания неприводимости*, в которой дан унитарный многочлен f степени n над $\mathbb{F}_p$ и требуется узнать, неприводим ли f над $\mathbb{F}_p$, есть эффективный алгоритм (тест Рабина, 1980).

Для задачи *распознавания неприводимости*, в которой дан унитарный многочлен f степени n над $\mathbb{F}_p$ и требуется узнать, неприводим ли f над $\mathbb{F}_p$, есть эффективный алгоритм (тест Рабина, 1980). Он допускает имплементацию за время $O(n^2 \log n \log p)$ при условии, что известно разложение числа n на простые множители.

Для задачи *распознавания неприводимости*, в которой дан унитарный многочлен f степени n над $\mathbb{F}_p$ и требуется узнать, неприводим ли f над $\mathbb{F}_p$, есть эффективный алгоритм (тест Рабина, 1980). Он допускает имплементацию за время $O(n^2 \log n \log p)$ при условии, что известно разложение числа n на простые множители.

Для задачи *факторизации* над $\mathbb{F}_p$, в которой дан многочлен f степени n над $\mathbb{F}_p$ и требуется разложить f на неприводимые над $\mathbb{F}_p$ множители, существуют достаточно эффективные *рандомизированные* алгоритмы, среднее время работы которых полиномиально зависит от n и $\log p$ (например, алгоритм Кантора–Цассенхауза, 1981, для нечетных p).

Для задачи *распознавания неприводимости*, в которой дан унитарный многочлен f степени n над $\mathbb{F}_p$ и требуется узнать, неприводим ли f над $\mathbb{F}_p$, есть эффективный алгоритм (тест Рабина, 1980). Он допускает имплементацию за время $O(n^2 \log n \log p)$ при условии, что известно разложение числа n на простые множители.

Для задачи *факторизации* над $\mathbb{F}_p$, в которой дан многочлен f степени n над $\mathbb{F}_p$ и требуется разложить f на неприводимые над $\mathbb{F}_p$ множители, существуют достаточно эффективные *рандомизированные* алгоритмы, среднее время работы которых полиномиально зависит от n и $\log p$ (например, алгоритм Кантора–Цассенхауза, 1981, для нечетных p). Имеется также *детерминированный* алгоритм со средним временем работы, полиномиальным от n и $\log p$, но требующий $O(n^2\sqrt{p})$ времени в худшем случае (алгоритм Шоупа, 1990).

Разложение на неприводимые множители над $\mathbb{F}_p$

Для задачи *распознавания неприводимости*, в которой дан унитарный многочлен f степени n над $\mathbb{F}_p$ и требуется узнать, неприводим ли f над $\mathbb{F}_p$, есть эффективный алгоритм (тест Рабина, 1980). Он допускает имплементацию за время $O(n^2 \log n \log p)$ при условии, что известно разложение числа n на простые множители.

Для задачи *факторизации* над $\mathbb{F}_p$, в которой дан многочлен f степени n над $\mathbb{F}_p$ и требуется разложить f на неприводимые над $\mathbb{F}_p$ множители, существуют достаточно эффективные *рандомизированные* алгоритмы, среднее время работы которых полиномиально зависит от n и $\log p$ (например, алгоритм Кантора–Цассенхауза, 1981, для нечетных p). Имеется также *детерминированный* алгоритм со средним временем работы, полиномиальным от n и $\log p$, но требующий $O(n^2\sqrt{p})$ времени в худшем случае (алгоритм Шоупа, 1990). Вопрос о существовании детерминированного алгоритма, гарантированно работающего за время, полиномиальное от n и $\log p$, является важной *открытой проблемой*.