ТЕОРЕМА ГАУССА О РАЗРЕШИМОСТИ В РАДИКАЛАХ

Рассмотрим калькулятор с кнопками

$$1, \quad +, \quad -, \quad \times, \quad : \quad \text{и} \quad \sqrt{}.$$

Калькулятор вычисляет числа с абсолютной точностью и имеет неограниченную память. При делении на 0 он выдает ошибку.

ТЕОРЕМА ГАУССА О РАЗРЕШИМОСТИ В РАДИКАЛАХ

Рассмотрим калькулятор с кнопками

$$1, \quad +, \quad -, \quad \times, \quad : \quad \text{и} \quad \sqrt{}.$$

Калькулятор вычисляет числа с абсолютной точностью и имеет неограниченную память. При делении на 0 он выдает ошибку.
Пусть сначала калькулятор *вещественный*, т.е. оперирует с вещественными числами и при извлечении корня четной степени из отрицательного числа выдает ошибку.

ТЕОРЕМА ГАУССА О РАЗРЕШИМОСТИ В РАДИКАЛАХ

Рассмотрим калькулятор с кнопками

$$1, \quad +, \quad -, \quad \times, \quad : \quad \text{и} \quad \sqrt{}.$$

Калькулятор вычисляет числа с абсолютной точностью и имеет неограниченную память. При делении на 0 он выдает ошибку.
Пусть сначала калькулятор *вещественный*, т.е. оперирует с вещественными числами и при извлечении корня четной степени из отрицательного числа выдает ошибку.
Вещественное число называется *вещественно построимым*, если его можно получить на вещественном калькуляторе так, чтобы при этом извлекались корни только второй степени (т.е. получить из 1 при помощи сложений, вычитаний, умножений, делений и извлечений квадратного корня из положительных чисел).

Например, вещественно построимы числа

$$\sqrt[4]{2} = \sqrt{\sqrt{2}}, \quad \sqrt{2\sqrt{3}}, \quad \sqrt{2} + \sqrt{3}, \quad \frac{1}{1+\sqrt{2}} \quad \text{и} \quad \cos 3^\circ.$$

Например, вещественно построимы числа

$$\sqrt[4]{2} = \sqrt{\sqrt{2}}, \quad \sqrt{2\sqrt{3}}, \quad \sqrt{2} + \sqrt{3}, \quad \frac{1}{1+\sqrt{2}} \quad \text{и} \quad \cos 3^\circ.$$

Теорема Гаусса. *Число* $\cos \dfrac{2\pi}{n}$ *вещественно построимо тогда и только тогда, когда* $n = 2^\alpha p_1 \dots p_l$, *где* $p_1, \dots, p_l$ — *различные простые числа вида* $2^{2^s} + 1$.

Например, вещественно построимы числа

$$\sqrt[4]{2} = \sqrt{\sqrt{2}}, \quad \sqrt{2\sqrt{3}}, \quad \sqrt{2} + \sqrt{3}, \quad \frac{1}{1+\sqrt{2}} \quad \text{и} \quad \cos 3^\circ.$$

Теорема Гаусса. *Число* $\cos\dfrac{2\pi}{n}$ *вещественно построимо тогда и только тогда, когда* $n = 2^\alpha p_1 \dots p_l$, *где* $p_1, \dots, p_l$ — *различные простые числа вида* $2^{2^s} + 1$.

Теорему Гаусса можно переформулировать в терминах *построимости циркулем и линейкой* правильных многоугольников.

Например, вещественно построимы числа

$$\sqrt[4]{2} = \sqrt{\sqrt{2}}, \quad \sqrt{2\sqrt{3}}, \quad \sqrt{2} + \sqrt{3}, \quad \frac{1}{1+\sqrt{2}} \quad \text{и} \quad \cos 3^\circ.$$

Теорема Гаусса. *Число* $\cos\dfrac{2\pi}{n}$ *вещественно построимо тогда и только тогда, когда* $n = 2^\alpha p_1 \dots p_l$, *где* $p_1, \dots, p_l$ — *различные простые числа вида* $2^{2^s}+1$.

Теорему Гаусса можно переформулировать в терминах *построимости циркулем и линейкой* правильных многоугольников.

Строго говоря, теорема Гаусса не дает настоящего решения проблемы построимости, поскольку неизвестно, какие числа вида $2^{2^s}+1$ являются простыми. Однако теорема Гаусса дает, например, быстрый алгоритм выяснения построимости числа $\cos\dfrac{2\pi}{n}$.

История этой знаменитой теоремы здесь не приводится, см. книгу С. Гиндикина.
Эта теорема интересна современному человеку как решение пробной задачи об *исследовании операций*.

История этой знаменитой теоремы здесь не приводится, см. книгу С. Гиндикина.
Эта теорема интересна современному человеку как решение пробной задачи об *исследовании операций*.
Здесь будет приведено малоизвестное простое элементарное доказательство приведенной теоремы. Оно получено из содержащегося в книге Г. Эдвардса ‘Теория Галуа’ некоторым упрощением.

История этой знаменитой теоремы здесь не приводится, см. книгу С. Гиндикина.
Эта теорема интересна современному человеку как решение пробной задачи об *исследовании операций*.
Здесь будет приведено малоизвестное простое элементарное доказательство приведенной теоремы. Оно получено из содержащегося в книге Г. Эдвардса ‘Теория Галуа’ некоторым упрощением.
Комплексный калькулятор имеет те же кнопки, что и вещественный, но оперирует с комплексными числами и при нажатии кнопки $\sqrt{}$ выдает оба значения корня.

История этой знаменитой теоремы здесь не приводится, см. книгу С. Гиндикина.
Эта теорема интересна современному человеку как решение пробной задачи об *исследовании операций*.
Здесь будет приведено малоизвестное простое элементарное доказательство приведенной теоремы. Оно получено из содержащегося в книге Г. Эдвардса ‘Теория Галуа’ некоторым упрощением.
Комплексный калькулятор имеет те же кнопки, что и вещественный, но оперирует с комплексными числами и при нажатии кнопки $\sqrt{}$ выдает оба значения корня.
На (комплексном или вещественном) калькуляторе можно получить число, если на нем можно получить *множество* чисел, содержащих заданное число.

Комплексное число называется *построимым*, если его можно получить на комплексном калькуляторе.

Комплексное число называется *построимым*, если его можно получить на комплексном калькуляторе.

Лемма о комплексификации. *Комплексное число построимо тогда и только тогда, когда его вещественная и мнимая части вещественно построимы.*

Комплексное число называется *построимым*, если его можно получить на комплексном калькуляторе.

Лемма о комплексификации. *Комплексное число построимо тогда и только тогда, когда его вещественная и мнимая части вещественно построимы.*

Указание к доказательству. Часть ‘тогда’ очевидна.

Комплексное число называется *построимым*, если его можно получить на комплексном калькуляторе.

Лемма о комплексификации. *Комплексное число построимо тогда и только тогда, когда его вещественная и мнимая части вещественно построимы.*

Указание к доказательству. Часть ‘тогда’ очевидна. (Заметим, что на калькуляторе нет кнопок Re и Im.)

Комплексное число называется *построимым*, если его можно получить на комплексном калькуляторе.

Лемма о комплексификации. *Комплексное число построимо тогда и только тогда, когда его вещественная и мнимая части вещественно построимы.*

Указание к доказательству. Часть ‘тогда’ очевидна. (Заметим, что на калькуляторе нет кнопок *Re* и *Im*.) Для доказательства части ‘только тогда’ напишите $\sqrt{a+bi} = u+vi$ и выразите u, v через a и b с помощью четырех арифметических операций и квадратных радикалов. QED

Комплексное число называется *построимым*, если его можно получить на комплексном калькуляторе.

Лемма о комплексификации. *Комплексное число построимо тогда и только тогда, когда его вещественная и мнимая части вещественно построимы.*

Указание к доказательству. Часть ‘тогда’ очевидна. (Заметим, что на калькуляторе нет кнопок *Re* и *Im*.) Для доказательства части ‘только тогда’ напишите $\sqrt{a+bi} = u + vi$ и выразите u, v через a и b с помощью четырех арифметических операций и квадратных радикалов. QED

Лемма о комплексификации (продолжение). *Число* $\cos(2\pi/n)$ *построимо тогда и только тогда, когда число* $\varepsilon_n := \cos(2\pi/n) + i\sin(2\pi/n)$ *построимо.*

Доказательство построимости в теореме Гаусса.

Доказательство построимости в теореме Гаусса.

Лемма об умножении. *Если ε_n и ε_m построимы и m, n взаимно просты, то ε_{2n} и ε_{mn} построимы.*

Доказательство построимости в теореме Гаусса.

Лемма об умножении. *Если ε_n и ε_m построимы и m, n взаимно просты, то ε_{2n} и ε_{mn} построимы.*

Доказательство получается из формул $\varepsilon_{2n} \in \sqrt{\varepsilon_n}$ и $\varepsilon_{mn} = \varepsilon_m^x \varepsilon_n^y$, где x и y — целые числа, для которых $nx + my = 1$. QED

Доказательство построимости в теореме Гаусса.

Лемма об умножении. *Если ε_n и ε_m построимы и m, n взаимно просты, то ε_{2n} и ε_{mn} построимы.*

Доказательство получается из формул $\varepsilon_{2n} \in \sqrt{\varepsilon_n}$ и $\varepsilon_{mn} = \varepsilon_m^x \varepsilon_n^y$, где x и y — целые числа, для которых $nx + my = 1$. QED

Доказательство построимости в теореме Гаусса. По леммам о комплексификации и об умножении достаточно доказать, что ε_n построимо для простого $n = 2^{2^s} + 1$. Так как $n - 1 = 2^m$, то по лемме об умножении ε_{n-1} построимо. Значит, построимость числа ε_n вытекает из следующей леммы. QED

Доказательство построимости в теореме Гаусса.

Лемма об умножении. *Если ε_n и ε_m построимы и m, n взаимно просты, то ε_{2n} и ε_{mn} построимы.*

Доказательство получается из формул $\varepsilon_{2n} \in \sqrt{\varepsilon_n}$ и $\varepsilon_{mn} = \varepsilon_m^x \varepsilon_n^y$, где x и y — целые числа, для которых $nx + my = 1$. QED

Доказательство построимости в теореме Гаусса. По леммам о комплексификации и об умножении достаточно доказать, что ε_n построимо для простого $n = 2^{2^s} + 1$. Так как $n - 1 = 2^m$, то по лемме об умножении ε_{n-1} построимо. Значит, построимость числа ε_n вытекает из следующей леммы. QED

Основная Лемма. *Если n простое, то из чисел 1 и $\beta := \varepsilon_{n-1}$ можно получить множество чисел, содержащее $\varepsilon := \varepsilon_n$, используя четыре арифметические операции и извлечения корней $(n-1)$-й степени (при которых получаются все $n-1$ значений корня).*

Доказательство основной леммы для $n = 5$. Let

Доказательство основной леммы для $n = 5$. Let

$$
\begin{aligned}
T_0 :=& \varepsilon + \varepsilon^2 + \varepsilon^4 + \varepsilon^8 = -1, \\
T_1 :=& \varepsilon + i\varepsilon^2 - \varepsilon^4 - i\varepsilon^8, \\
T_2 :=& \varepsilon - \varepsilon^2 + \varepsilon^4 - \varepsilon^8 \qquad \text{and} \\
T_3 :=& \varepsilon - i\varepsilon^2 - \varepsilon^4 + i\varepsilon^8.
\end{aligned}
$$

Доказательство основной леммы для $n = 5$. Let

$$\begin{aligned} T_0 :=& \varepsilon + \varepsilon^2 + \varepsilon^4 + \varepsilon^8 = -1, \\ T_1 :=& \varepsilon + i\varepsilon^2 - \varepsilon^4 - i\varepsilon^8, \\ T_2 :=& \varepsilon - \varepsilon^2 + \varepsilon^4 - \varepsilon^8 \qquad \text{and} \\ T_3 :=& \varepsilon - i\varepsilon^2 - \varepsilon^4 + i\varepsilon^8. \end{aligned}$$

('Резольвенты Лагранжа'.) Тогда $T_0 + T_1 + T_2 + T_3 = 4\varepsilon$. Поэтому достаточно доказать лемму с заменой ε на каждое из чисел T_1, T_2, T_3.

Доказательство основной леммы для $n = 5$. Let

$$\begin{aligned} T_0 :=& \varepsilon + \varepsilon^2 + \varepsilon^4 + \varepsilon^8 = -1, \\ T_1 :=& \varepsilon + i\varepsilon^2 - \varepsilon^4 - i\varepsilon^8, \\ T_2 :=& \varepsilon - \varepsilon^2 + \varepsilon^4 - \varepsilon^8 \qquad \text{and} \\ T_3 :=& \varepsilon - i\varepsilon^2 - \varepsilon^4 + i\varepsilon^8. \end{aligned}$$

('Резольвенты Лагранжа'.) Тогда $T_0 + T_1 + T_2 + T_3 = 4\varepsilon$. Поэтому достаточно доказать лемму с заменой ε на каждое из чисел T_1, T_2, T_3.
Clearly, T_1 goes to $-iT_1$ under the substitution of ε to ε^2.

Доказательство основной леммы для $n = 5$. Let

$$\begin{aligned} T_0 :=& \varepsilon + \varepsilon^2 + \varepsilon^4 + \varepsilon^8 = -1, \\ T_1 :=& \varepsilon + i\varepsilon^2 - \varepsilon^4 - i\varepsilon^8, \\ T_2 :=& \varepsilon - \varepsilon^2 + \varepsilon^4 - \varepsilon^8 \qquad \text{and} \\ T_3 :=& \varepsilon - i\varepsilon^2 - \varepsilon^4 + i\varepsilon^8. \end{aligned}$$

('Резольвенты Лагранжа'.) Тогда $T_0 + T_1 + T_2 + T_3 = 4\varepsilon$. Поэтому достаточно доказать лемму с заменой ε на каждое из чисел T_1, T_2, T_3.
Clearly, T_1 goes to $-iT_1$ under the substitution of ε to ε^2. Hence T_1^4 is invariant under this substitution.

Доказательство основной леммы для $n = 5$. Let

$$\begin{aligned} T_0 :=& \varepsilon + \varepsilon^2 + \varepsilon^4 + \varepsilon^8 = -1, \\ T_1 :=& \varepsilon + i\varepsilon^2 - \varepsilon^4 - i\varepsilon^8, \\ T_2 :=& \varepsilon - \varepsilon^2 + \varepsilon^4 - \varepsilon^8 \qquad \text{and} \\ T_3 :=& \varepsilon - i\varepsilon^2 - \varepsilon^4 + i\varepsilon^8. \end{aligned}$$

('Резольвенты Лагранжа'.) Тогда $T_0 + T_1 + T_2 + T_3 = 4\varepsilon$. Поэтому достаточно доказать лемму с заменой ε на каждое из чисел T_1, T_2, T_3.
Clearly, T_1 goes to $-iT_1$ under the substitution of ε to ε^2. Hence T_1^4 is invariant under this substitution. Open brackets in the product T_1^4 and substitute ε^5 to 1. We obtain an equality

Доказательство основной леммы для $n = 5$. Let

$$\begin{aligned} T_0 :=& \varepsilon + \varepsilon^2 + \varepsilon^4 + \varepsilon^8 = -1, \\ T_1 :=& \varepsilon + i\varepsilon^2 - \varepsilon^4 - i\varepsilon^8, \\ T_2 :=& \varepsilon - \varepsilon^2 + \varepsilon^4 - \varepsilon^8 \qquad \text{and} \\ T_3 :=& \varepsilon - i\varepsilon^2 - \varepsilon^4 + i\varepsilon^8. \end{aligned}$$

('Резольвенты Лагранжа'.) Тогда $T_0 + T_1 + T_2 + T_3 = 4\varepsilon$. Поэтому достаточно доказать лемму с заменой ε на каждое из чисел T_1, T_2, T_3.
Clearly, T_1 goes to $-iT_1$ under the substitution of ε to ε^2. Hence T_1^4 is invariant under this substitution. Open brackets in the product T_1^4 and substitute ε^5 to 1. We obtain an equality

$$T_1^4 = a_0 + a_1\varepsilon + a_2\varepsilon^2 + a_3\varepsilon^3 + a_4\varepsilon^4 \quad \text{for some} \quad a_k \in \mathbb{Z} + i\mathbb{Z}.$$

Доказательство основной леммы для $n = 5$. Let

$$\begin{aligned} T_0 :=& \varepsilon + \varepsilon^2 + \varepsilon^4 + \varepsilon^8 = -1, \\ T_1 :=& \varepsilon + i\varepsilon^2 - \varepsilon^4 - i\varepsilon^8, \\ T_2 :=& \varepsilon - \varepsilon^2 + \varepsilon^4 - \varepsilon^8 \qquad \text{and} \\ T_3 :=& \varepsilon - i\varepsilon^2 - \varepsilon^4 + i\varepsilon^8. \end{aligned}$$

('Резольвенты Лагранжа'.) Тогда $T_0 + T_1 + T_2 + T_3 = 4\varepsilon$. Поэтому достаточно доказать лемму с заменой ε на каждое из чисел T_1, T_2, T_3.
Clearly, T_1 goes to $-iT_1$ under the substitution of ε to ε^2. Hence T_1^4 is invariant under this substitution. Open brackets in the product T_1^4 and substitute ε^5 to 1. We obtain an equality

$$T_1^4 = a_0 + a_1\varepsilon + a_2\varepsilon^2 + a_3\varepsilon^3 + a_4\varepsilon^4 \quad \text{for some} \quad a_k \in \mathbb{Z} + i\mathbb{Z}.$$

Since T_1^4 is invariant under substitution of ε to ε^2, we have $a_1 = a_2 = a_4 = a_3$.

Доказательство основной леммы для $n = 5$. Let

$$\begin{aligned} T_0 :=& \varepsilon + \varepsilon^2 + \varepsilon^4 + \varepsilon^8 = -1, \\ T_1 :=& \varepsilon + i\varepsilon^2 - \varepsilon^4 - i\varepsilon^8, \\ T_2 :=& \varepsilon - \varepsilon^2 + \varepsilon^4 - \varepsilon^8 \qquad \text{and} \\ T_3 :=& \varepsilon - i\varepsilon^2 - \varepsilon^4 + i\varepsilon^8. \end{aligned}$$

('Резольвенты Лагранжа'.) Тогда $T_0 + T_1 + T_2 + T_3 = 4\varepsilon$. Поэтому достаточно доказать лемму с заменой ε на каждое из чисел T_1, T_2, T_3.
Clearly, T_1 goes to $-iT_1$ under the substitution of ε to ε^2. Hence T_1^4 is invariant under this substitution. Open brackets in the product T_1^4 and substitute ε^5 to 1. We obtain an equality

$$T_1^4 = a_0 + a_1\varepsilon + a_2\varepsilon^2 + a_3\varepsilon^3 + a_4\varepsilon^4 \quad \text{for some} \quad a_k \in \mathbb{Z} + i\mathbb{Z}.$$

Since T_1^4 is invariant under substitution of ε to ε^2, we have $a_1 = a_2 = a_4 = a_3$. Therefore $T_1^4 = a_0 - a_1 \in \mathbb{Z} + i\mathbb{Z}$.

Доказательство основной леммы для $n = 5$. Let

$$\begin{aligned} T_0 :=& \varepsilon + \varepsilon^2 + \varepsilon^4 + \varepsilon^8 = -1, \\ T_1 :=& \varepsilon + i\varepsilon^2 - \varepsilon^4 - i\varepsilon^8, \\ T_2 :=& \varepsilon - \varepsilon^2 + \varepsilon^4 - \varepsilon^8 \qquad \text{and} \\ T_3 :=& \varepsilon - i\varepsilon^2 - \varepsilon^4 + i\varepsilon^8. \end{aligned}$$

('Резольвенты Лагранжа'.) Тогда $T_0 + T_1 + T_2 + T_3 = 4\varepsilon$. Поэтому достаточно доказать лемму с заменой ε на каждое из чисел T_1, T_2, T_3.
Clearly, T_1 goes to $-iT_1$ under the substitution of ε to ε^2. Hence T_1^4 is invariant under this substitution. Open brackets in the product T_1^4 and substitute ε^5 to 1. We obtain an equality

$$T_1^4 = a_0 + a_1\varepsilon + a_2\varepsilon^2 + a_3\varepsilon^3 + a_4\varepsilon^4 \quad \text{for some} \quad a_k \in \mathbb{Z} + i\mathbb{Z}.$$

Since T_1^4 is invariant under substitution of ε to ε^2, we have $a_1 = a_2 = a_4 = a_3$. Therefore $T_1^4 = a_0 - a_1 \in \mathbb{Z} + i\mathbb{Z}$. Thus Lemma holds for T_1.

Доказательство основной леммы для $n = 5$. Let

$$\begin{aligned} T_0 :=& \varepsilon + \varepsilon^2 + \varepsilon^4 + \varepsilon^8 = -1, \\ T_1 :=& \varepsilon + i\varepsilon^2 - \varepsilon^4 - i\varepsilon^8, \\ T_2 :=& \varepsilon - \varepsilon^2 + \varepsilon^4 - \varepsilon^8 \qquad \text{and} \\ T_3 :=& \varepsilon - i\varepsilon^2 - \varepsilon^4 + i\varepsilon^8. \end{aligned}$$

('Резольвенты Лагранжа'.) Тогда $T_0 + T_1 + T_2 + T_3 = 4\varepsilon$. Поэтому достаточно доказать лемму с заменой ε на каждое из чисел T_1, T_2, T_3.
Clearly, T_1 goes to $-iT_1$ under the substitution of ε to ε^2. Hence T_1^4 is invariant under this substitution. Open brackets in the product T_1^4 and substitute ε^5 to 1. We obtain an equality

$$T_1^4 = a_0 + a_1\varepsilon + a_2\varepsilon^2 + a_3\varepsilon^3 + a_4\varepsilon^4 \quad \text{for some} \quad a_k \in \mathbb{Z} + i\mathbb{Z}.$$

Since T_1^4 is invariant under substitution of ε to ε^2, we have $a_1 = a_2 = a_4 = a_3$. Therefore $T_1^4 = a_0 - a_1 \in \mathbb{Z} + i\mathbb{Z}$. Thus Lemma holds for T_1. Analogously it holds for T_2 and T_3.

В приведенном рассуждении нужно обосновать вывод ‘$a_1 = a_2 = a_4 = a_3$’. Вместо этого изменим немного доказательство.

В приведенном рассуждении нужно обосновать вывод ‘$a_1 = a_2 = a_4 = a_3$’. Вместо этого изменим немного доказательство. Определим многочлен $T_1(x) := x + ix^2 - x^4 - ix^8$.

В приведенном рассуждении нужно обосновать вывод ‘$a_1 = a_2 = a_4 = a_3$’. Вместо этого изменим немного доказательство. Определим многочлен $T_1(x) := x + ix^2 - x^4 - ix^8$. Определим многочлены $T_0(x)$, $T_2(x)$ и $T_3(x)$ формулами, аналогичными вышенаписанным.

В приведенном рассуждении нужно обосновать вывод ‘$a_1 = a_2 = a_4 = a_3$’. Вместо этого изменим немного доказательство. Определим многочлен $T_1(x) := x + ix^2 - x^4 - ix^8$. Определим многочлены $T_0(x)$, $T_2(x)$ и $T_3(x)$ формулами, аналогичными вышенаписанным. Как и выше, $(T_0 + T_1 + T_2 + T_3)(\varepsilon) = 4\varepsilon$.

В приведенном рассуждении нужно обосновать вывод ‘$a_1 = a_2 = a_4 = a_3$’. Вместо этого изменим немного доказательство. Определим многочлен $T_1(x) := x + ix^2 - x^4 - ix^8$. Определим многочлены $T_0(x)$, $T_2(x)$ и $T_3(x)$ формулами, аналогичными вышенаписанным. Как и выше, $(T_0 + T_1 + T_2 + T_3)(\varepsilon) = 4\varepsilon$. Поэтому достаточно доказать лемму с заменой ε на каждое из чисел $T_r(\varepsilon)$, $r = 1, 2, 3$.

В приведенном рассуждении нужно обосновать вывод ‘$a_1 = a_2 = a_4 = a_3$’. Вместо этого изменим немного доказательство. Определим многочлен $T_1(x) := x + ix^2 - x^4 - ix^8$. Определим многочлены $T_0(x)$, $T_2(x)$ и $T_3(x)$ формулами, аналогичными вышенаписанным. Как и выше, $(T_0 + T_1 + T_2 + T_3)(\varepsilon) = 4\varepsilon$. Поэтому достаточно доказать лемму с заменой ε на каждое из чисел $T_r(\varepsilon)$, $r = 1, 2, 3$. Так как

$$iT_1(x^2) \equiv T_1(x) \mod (x^5 - 1), \quad \text{то}$$
$$T_1^4(x^2) \equiv T_1^4(x) \mod (x^5 - 1).$$

Возьмем многочлен $a_0 + a_1x + a_2x^2 + a_3x^3 + a_4x^4$ с коэффициентами в $\mathbb{Z}[i]$, сравнимый с $T_1^4(x)$ по модулю $x^5 - 1$.

В приведенном рассуждении нужно обосновать вывод ‘$a_1 = a_2 = a_4 = a_3$’. Вместо этого изменим немного доказательство. Определим многочлен $T_1(x) := x + ix^2 - x^4 - ix^8$. Определим многочлены $T_0(x)$, $T_2(x)$ и $T_3(x)$ формулами, аналогичными вышенаписанным. Как и выше, $(T_0 + T_1 + T_2 + T_3)(\varepsilon) = 4\varepsilon$. Поэтому достаточно доказать лемму с заменой ε на каждое из чисел $T_r(\varepsilon)$, $r = 1, 2, 3$. Так как

$$iT_1(x^2) \equiv T_1(x) \mod (x^5 - 1), \quad \text{то}$$
$$T_1^4(x^2) \equiv T_1^4(x) \mod (x^5 - 1).$$

Возьмем многочлен $a_0 + a_1x + a_2x^2 + a_3x^3 + a_4x^4$ с коэффициентами в $\mathbb{Z}[i]$, сравнимый с $T_1^4(x)$ по модулю $x^5 - 1$. Тогда $a_k = a_{2k \mod 5}$ для любого $k = 1, 2, 3, 4$.

В приведенном рассуждении нужно обосновать вывод '$a_1 = a_2 = a_4 = a_3$'. Вместо этого изменим немного доказательство. Определим многочлен $T_1(x) := x + ix^2 - x^4 - ix^8$. Определим многочлены $T_0(x)$, $T_2(x)$ и $T_3(x)$ формулами, аналогичными вышенаписанным. Как и выше, $(T_0 + T_1 + T_2 + T_3)(\varepsilon) = 4\varepsilon$. Поэтому достаточно доказать лемму с заменой ε на каждое из чисел $T_r(\varepsilon)$, $r = 1, 2, 3$. Так как

$$iT_1(x^2) \equiv T_1(x) \mod (x^5 - 1), \quad \text{то}$$
$$T_1^4(x^2) \equiv T_1^4(x) \mod (x^5 - 1).$$

Возьмем многочлен $a_0 + a_1x + a_2x^2 + a_3x^3 + a_4x^4$ с коэффициентами в $\mathbb{Z}[i]$, сравнимый с $T_1^4(x)$ по модулю $x^5 - 1$. Тогда $a_k = a_{2k} \mod 5$ для любого $k = 1, 2, 3, 4$. Значит, $a_1 = a_2 = a_4 = a_3$.

В приведенном рассуждении нужно обосновать вывод ‘$a_1 = a_2 = a_4 = a_3$’. Вместо этого изменим немного доказательство. Определим многочлен $T_1(x) := x + ix^2 - x^4 - ix^8$. Определим многочлены $T_0(x)$, $T_2(x)$ и $T_3(x)$ формулами, аналогичными вышенаписанным. Как и выше, $(T_0 + T_1 + T_2 + T_3)(\varepsilon) = 4\varepsilon$. Поэтому достаточно доказать лемму с заменой ε на каждое из чисел $T_r(\varepsilon)$, $r = 1, 2, 3$. Так как

$$iT_1(x^2) \equiv T_1(x) \mod (x^5 - 1), \quad \text{то}$$
$$T_1^4(x^2) \equiv T_1^4(x) \mod (x^5 - 1).$$

Возьмем многочлен $a_0 + a_1x + a_2x^2 + a_3x^3 + a_4x^4$ с коэффициентами в $\mathbb{Z}[i]$, сравнимый с $T_1^4(x)$ по модулю $x^5 - 1$. Тогда $a_k = a_{2k} \mod 5$ для любого $k = 1, 2, 3, 4$. Значит, $a_1 = a_2 = a_4 = a_3$. Поэтому $T_1^4(\varepsilon) = a_0 - a_1 \in \mathbb{Z}[i]$.

В приведенном рассуждении нужно обосновать вывод '$a_1 = a_2 = a_4 = a_3$'. Вместо этого изменим немного доказательство. Определим многочлен $T_1(x) := x + ix^2 - x^4 - ix^8$. Определим многочлены $T_0(x)$, $T_2(x)$ и $T_3(x)$ формулами, аналогичными вышенаписанным. Как и выше, $(T_0 + T_1 + T_2 + T_3)(\varepsilon) = 4\varepsilon$. Поэтому достаточно доказать лемму с заменой ε на каждое из чисел $T_r(\varepsilon)$, $r = 1, 2, 3$. Так как

$$iT_1(x^2) \equiv T_1(x) \mod (x^5 - 1), \quad \text{то}$$
$$T_1^4(x^2) \equiv T_1^4(x) \mod (x^5 - 1).$$

Возьмем многочлен $a_0 + a_1x + a_2x^2 + a_3x^3 + a_4x^4$ с коэффициентами в $\mathbb{Z}[i]$, сравнимый с $T_1^4(x)$ по модулю $x^5 - 1$. Тогда $a_k = a_{2k} \mod 5$ для любого $k = 1, 2, 3, 4$. Значит, $a_1 = a_2 = a_4 = a_3$. Поэтому $T_1^4(\varepsilon) = a_0 - a_1 \in \mathbb{Z}[i]$. Значит, лемма верна для числа $T_1(\varepsilon)$.

В приведенном рассуждении нужно обосновать вывод ‘$a_1 = a_2 = a_4 = a_3$’. Вместо этого изменим немного доказательство. Определим многочлен $T_1(x) := x + ix^2 - x^4 - ix^8$. Определим многочлены $T_0(x)$, $T_2(x)$ и $T_3(x)$ формулами, аналогичными вышенаписанным. Как и выше, $(T_0 + T_1 + T_2 + T_3)(\varepsilon) = 4\varepsilon$. Поэтому достаточно доказать лемму с заменой ε на каждое из чисел $T_r(\varepsilon)$, $r = 1, 2, 3$. Так как

$$iT_1(x^2) \equiv T_1(x) \mod (x^5 - 1), \quad \text{то}$$
$$T_1^4(x^2) \equiv T_1^4(x) \mod (x^5 - 1).$$

Возьмем многочлен $a_0 + a_1x + a_2x^2 + a_3x^3 + a_4x^4$ с коэффициентами в $\mathbb{Z}[i]$, сравнимый с $T_1^4(x)$ по модулю $x^5 - 1$. Тогда $a_k = a_{2k} \mod 5$ для любого $k = 1, 2, 3, 4$. Значит, $a_1 = a_2 = a_4 = a_3$. Поэтому $T_1^4(\varepsilon) = a_0 - a_1 \in \mathbb{Z}[i]$. Значит, лемма верна для числа $T_1(\varepsilon)$. Аналогично она верна для чисел $T_2(\varepsilon)$ и $T_3(\varepsilon)$. QED

Теорема о первообразном корне. *Для любого простого p существует число g, для которого остатки от деления на p чисел $g^1, g^2, g^3, \ldots, g^{p-1}$ различны.*

Теорема о первообразном корне. *Для любого простого p существует число g, для которого остатки от деления на p чисел $g^1, g^2, g^3, \ldots, g^{p-1}$ различны.*

Указание к доказательству для $p = 2^m + 1$ (только этот случай нужен для теоремы Гаусса).

Теорема о первообразном корне. *Для любого простого p существует число g, для которого остатки от деления на p чисел $g^1, g^2, g^3, \ldots, g^{p-1}$ различны.*

Указание к доказательству для $p = 2^m + 1$ (только этот случай нужен для теоремы Гаусса). Если первообразного корня нет, то сравнение $x^{2^{m-1}} \equiv 1 \bmod p$ имеет $p - 1 = 2^m > 2^{m-1}$ решений. QED

Доказательство основной леммы для общего случая. Пусть g — первообразный корень по модулю n.

Доказательство основной леммы для общего случая. Пусть g — первообразный корень по модулю n. Для $r = 0, 1, 2, \ldots, n-2$, обозначим

$$T_r(x) := x + \beta^r x^g + \beta^{2r} x^{g^2} + \cdots + \beta^{(n-2)r} x^{g^{n-2}} \in \mathbb{Z}[\beta][x].$$

(‘Резольвенты Лагранжа’.)

Доказательство основной леммы для общего случая. Пусть g — первообразный корень по модулю n. Для $r = 0, 1, 2, \ldots, n-2$, обозначим

$$T_r(x) := x + \beta^r x^g + \beta^{2r} x^{g^2} + \cdots + \beta^{(n-2)r} x^{g^{n-2}} \in \mathbb{Z}[\beta][x].$$

(‘Резольвенты Лагранжа’.) Тогда

$$(T_0 + T_1 + \cdots + T_{n-2})(\varepsilon) = (n-1)\varepsilon.$$

Доказательство основной леммы для общего случая. Пусть g — первообразный корень по модулю n. Для $r = 0, 1, 2, \ldots, n-2$, обозначим

$$T_r(x) := x + \beta^r x^g + \beta^{2r} x^{g^2} + \cdots + \beta^{(n-2)r} x^{g^{n-2}} \in \mathbb{Z}[\beta][x].$$

(‘Резольвенты Лагранжа’.) Тогда

$$(T_0 + T_1 + \cdots + T_{n-2})(\varepsilon) = (n-1)\varepsilon.$$

Имеем $T_0(\varepsilon) = -1$. Поэтому достаточно доказать лемму с заменой ε на каждое из чисел $T_r(\varepsilon)$, $r = 1, 2, \ldots, n-2$.

Доказательство основной леммы для общего случая. Пусть g — первообразный корень по модулю n. Для $r = 0, 1, 2, \ldots, n-2$, обозначим

$$T_r(x) := x + \beta^r x^g + \beta^{2r} x^{g^2} + \cdots + \beta^{(n-2)r} x^{g^{n-2}} \in \mathbb{Z}[\beta][x].$$

('Резольвенты Лагранжа'.) Тогда

$$(T_0 + T_1 + \cdots + T_{n-2})(\varepsilon) = (n-1)\varepsilon.$$

Имеем $T_0(\varepsilon) = -1$. Поэтому достаточно доказать лемму с заменой ε на каждое из чисел $T_r(\varepsilon)$, $r = 1, 2, \ldots, n-2$. Так как

$$\beta^r T_r(x^g) \equiv T_r(x) \mod (x^n - 1), \quad \text{то}$$
$$T_r^{n-1}(x^g) \equiv T_r^{n-1}(x) \mod (x^n - 1).$$

Доказательство основной леммы для общего случая. Пусть g — первообразный корень по модулю n. Для $r = 0, 1, 2, \ldots, n-2$, обозначим

$$T_r(x) := x + \beta^r x^g + \beta^{2r} x^{g^2} + \cdots + \beta^{(n-2)r} x^{g^{n-2}} \in \mathbb{Z}[\beta][x].$$

('Резольвенты Лагранжа'.) Тогда

$$(T_0 + T_1 + \cdots + T_{n-2})(\varepsilon) = (n-1)\varepsilon.$$

Имеем $T_0(\varepsilon) = -1$. Поэтому достаточно доказать лемму с заменой ε на каждое из чисел $T_r(\varepsilon)$, $r = 1, 2, \ldots, n-2$. Так как

$$\beta^r T_r(x^g) \equiv T_r(x) \mod (x^n - 1), \quad \text{то}$$
$$T_r^{n-1}(x^g) \equiv T_r^{n-1}(x) \mod (x^n - 1).$$

Возьмем многочлен $a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1} x^{n-1}$ с коэффициентами в $\mathbb{Z}[\beta]$, сравнимый с $T_r^{n-1}(x)$ по модулю $x^n - 1$.

Доказательство основной леммы для общего случая. Пусть g — первообразный корень по модулю n. Для $r = 0, 1, 2, \ldots, n-2$, обозначим

$$T_r(x) := x + \beta^r x^g + \beta^{2r} x^{g^2} + \cdots + \beta^{(n-2)r} x^{g^{n-2}} \in \mathbb{Z}[\beta][x].$$

(‘Резольвенты Лагранжа’.) Тогда

$$(T_0 + T_1 + \cdots + T_{n-2})(\varepsilon) = (n-1)\varepsilon.$$

Имеем $T_0(\varepsilon) = -1$. Поэтому достаточно доказать лемму с заменой ε на каждое из чисел $T_r(\varepsilon)$, $r = 1, 2, \ldots, n-2$. Так как

$$\beta^r T_r(x^g) \equiv T_r(x) \mod (x^n - 1), \quad \text{то}$$
$$T_r^{n-1}(x^g) \equiv T_r^{n-1}(x) \mod (x^n - 1).$$

Возьмем многочлен $a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1} x^{n-1}$ с коэффициентами в $\mathbb{Z}[\beta]$, сравнимый с $T_r^{n-1}(x)$ по модулю $x^n - 1$. Тогда $a_1 = a_g = a_{g^2} \mod n = a_{g^3} \mod n = \ldots$

Доказательство основной леммы для общего случая. Пусть g — первообразный корень по модулю n. Для $r = 0, 1, 2, \ldots, n-2$, обозначим

$$T_r(x) := x + \beta^r x^g + \beta^{2r} x^{g^2} + \cdots + \beta^{(n-2)r} x^{g^{n-2}} \in \mathbb{Z}[\beta][x].$$

('Резольвенты Лагранжа'.) Тогда

$$(T_0 + T_1 + \cdots + T_{n-2})(\varepsilon) = (n-1)\varepsilon.$$

Имеем $T_0(\varepsilon) = -1$. Поэтому достаточно доказать лемму с заменой ε на каждое из чисел $T_r(\varepsilon)$, $r = 1, 2, \ldots, n-2$. Так как

$$\beta^r T_r(x^g) \equiv T_r(x) \mod (x^n - 1), \quad \text{то}$$
$$T_r^{n-1}(x^g) \equiv T_r^{n-1}(x) \mod (x^n - 1).$$

Возьмем многочлен $a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1} x^{n-1}$ с коэффициентами в $\mathbb{Z}[\beta]$, сравнимый с $T_r^{n-1}(x)$ по модулю $x^n - 1$. Тогда $a_1 = a_g = a_{g^2 \bmod n} = a_{g^3 \bmod n} = \ldots$ Значит, $a_1 = a_2 = \cdots = a_{n-1}$.

Доказательство основной леммы для общего случая. Пусть g — первообразный корень по модулю n. Для $r = 0, 1, 2, \ldots, n-2$, обозначим

$$T_r(x) := x + \beta^r x^g + \beta^{2r} x^{g^2} + \cdots + \beta^{(n-2)r} x^{g^{n-2}} \in \mathbb{Z}[\beta][x].$$

('Резольвенты Лагранжа'.) Тогда

$$(T_0 + T_1 + \cdots + T_{n-2})(\varepsilon) = (n-1)\varepsilon.$$

Имеем $T_0(\varepsilon) = -1$. Поэтому достаточно доказать лемму с заменой ε на каждое из чисел $T_r(\varepsilon)$, $r = 1, 2, \ldots, n-2$. Так как

$$\beta^r T_r(x^g) \equiv T_r(x) \mod (x^n - 1), \quad \text{то}$$
$$T_r^{n-1}(x^g) \equiv T_r^{n-1}(x) \mod (x^n - 1).$$

Возьмем многочлен $a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1} x^{n-1}$ с коэффициентами в $\mathbb{Z}[\beta]$, сравнимый с $T_r^{n-1}(x)$ по модулю $x^n - 1$. Тогда $a_1 = a_g = a_{g^2 \bmod n} = a_{g^3 \bmod n} = \ldots$ Значит, $a_1 = a_2 = \cdots = a_{n-1}$. Поэтому $T_r^{n-1}(\varepsilon) = a_0 - a_1 \in \mathbb{Z}[\beta]$.

Доказательство основной леммы для общего случая. Пусть g — первообразный корень по модулю n. Для $r = 0, 1, 2, \ldots, n-2$, обозначим

$$T_r(x) := x + \beta^r x^g + \beta^{2r} x^{g^2} + \cdots + \beta^{(n-2)r} x^{g^{n-2}} \in \mathbb{Z}[\beta][x].$$

('Резольвенты Лагранжа'.) Тогда

$$(T_0 + T_1 + \cdots + T_{n-2})(\varepsilon) = (n-1)\varepsilon.$$

Имеем $T_0(\varepsilon) = -1$. Поэтому достаточно доказать лемму с заменой ε на каждое из чисел $T_r(\varepsilon)$, $r = 1, 2, \ldots, n-2$. Так как

$$\beta^r T_r(x^g) \equiv T_r(x) \mod (x^n - 1), \quad \text{то}$$
$$T_r^{n-1}(x^g) \equiv T_r^{n-1}(x) \mod (x^n - 1).$$

Возьмем многочлен $a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1} x^{n-1}$ с коэффициентами в $\mathbb{Z}[\beta]$, сравнимый с $T_r^{n-1}(x)$ по модулю $x^n - 1$. Тогда $a_1 = a_g = a_{g^2 \bmod n} = a_{g^3 \bmod n} = \ldots$ Значит, $a_1 = a_2 = \cdots = a_{n-1}$. Поэтому $T_r^{n-1}(\varepsilon) = a_0 - a_1 \in \mathbb{Z}[\beta]$. Значит, лемма верна с заменой ε на $T_r(\varepsilon)$. QED

Задача. (а) Приведите вычисление на комплексном калькуляторе числа ε_7, при котором извлекаются только корни второй и третьей степени. Сколько раз при этом извлекается корень третьей степени?

Задача. (a) Приведите вычисление на комплексном калькуляторе числа ε_7, при котором извлекаются только корни второй и третьей степени. Сколько раз при этом извлекается корень третьей степени?
(b) Докажите, что на комплексном калькуляторе можно получить число ε_7 так, чтобы только один раз извлекать корень третьей степени и не извлекать корней большей степени.

Задача. (a) Приведите вычисление на комплексном калькуляторе числа ε_7, при котором извлекаются только корни второй и третьей степени. Сколько раз при этом извлекается корень третьей степени?
(b) Докажите, что на комплексном калькуляторе можно получить число ε_7 так, чтобы только один раз извлекать корень третьей степени и не извлекать корней большей степени.

Задача для исследования. Для каких n число $\cos(2\pi/n)$
(a) рационально?
(b)* представимо в виде $a + \sqrt{b}$, где $a, b \in \mathbb{Q}$?
(c)* можно получить на вещественном калькуляторе, если разрешается извлекать корни *любых* степеней, а не только квадратные?