Чисел Кармайкла бесконечно много

Определение

Числа Кармайкла

Для любого числа a и простого n $a^n \ mod \ n = a$. Но это может быть верно и для составных n. Такие n и называются числами Кармайкла.

Критерий Корсельта

Число является числом Кармайкла тогда и только тогда, когда : 1)Оно свободно от квадратов. 2)Для любого p - простого делителя n $p-1$ делит $n-1$.

Результаты аналитической теории чисел

Теорема 1

Пусть $\pi(x)$ - количество простых, не превосходящих x, $\pi(x,y)$ - количество простых $p \leq x$, таких что все простые делители числа $p-1$ не превосходят y. Тогда существует маленькая константа E, такая что $\pi(x, x^{1-E}) \geq C_E \pi(x)$. Гипотеза состоит в том, что любое число до 1 подходит на роль этой константы.

Теорема 2

Пусть $\pi(x,d,a)$ - количество простых чисел до x, сравнимых с a по модулю d. Тогда существует очень маленькое число B с таким свойством: Пусть x достаточно большое, $1 \leq d \leq \min(x^B, \frac{y}{x^{1-B}})$. Тогда $\pi(x,d,a) \geq \frac{\pi(y)}{2\phi(d)}$, если d не делится на множество чисел фиксированного размера, не меньших $log x$. Это значит, что во многих арифметических прогрессиях с не очень большим знаменателем простых чисел достаточно много. Гипотеза опять же состоит в том, что любое число до 1 подходит на роль этой константы.

ТЕОРЕМА

Пусть $C(x)$ - количество чисел Кармайкла, не превосходящих x. Тогда для любого $\epsilon > 0 C(x) > x^{BE-\epsilon}$ при достаточно больших x. Гипотезы дают $C(x) > x^{1-\epsilon}$ для любого ϵ, подстановка наилучших известных доказанных значений для B и E дает чуть-чуть больше чем $\frac{2}{7}$.

Комбинаторные леммы

Лемма 1

Пусть G - конечная абелева группа, $n(G)$ - минимальное число с таким свойством - из любых $n(G)$ чисел можно выбрать несколько (не 0) с произведением 1. Тривиальная оценка - $n(G) < |G| + 1$, но для групп, далеких от циклической, можно и точнее. А именно, пусть m - максимальный порядок элемента группы, тогда $n(G) < m(1 + log\frac{|G|}{m})$

Лемма 2

Пусть G - абелева группа, $r > t > n = n(G)$. Тогда из любых r элементов группы можно выбрать от $t - n$ до t с произведением 1, причем это можно сделать не менее чем $\frac{C_r^t}{C_r^n}$ способами.

Конструкция

Для начала мы хотим построить такое число L, которое имеет много делителей вида $p-1$ для простого p. Идейно это потому, что: мы найдем число n с просто большим числом делителей, а потом для каждого делителя d рассмотрим числа $dk+1$ для небольших k. Аналитические леммы обеспечат нам, что для каждого делителя среди них много простых. Тогда существует k, для которого среди чисел $dk+1$ много простых, а dk- делитель числа nk.
Далее мы хотим выбрать из этих делителе й много наборов $p_1, p_2, \ldots, p_k$, такой что $M = p_1 p_2 \cdots p_k = 1 \ mod \ L$, пользуясь комбинаторными леммами (они хорошо работают как раз с числами с большим числом маленьких делителей). Тогда $M-1$ делится на L, а L на $p-1$, и число M - число Кармайкла.