Делимость

Малый мехмат МГУ

7 ноября 2020 г.

Задача для затравки

Существует ли число вида $11\ldots11$, кратное 123456789?

Подсказка

Рассмотрим числа 1, 11, 111, . . .,

$\underbrace{11\ldots11}_{123456790}$.

Решение

Среди чисел $1, 11, 111, \ldots, \underbrace{11\ldots11}_{123456790}$ найдутся два, дающих одинаковый остаток при делении на 123456789 (принцип Дирихле). Тогда их разность делится на 123456789. Но их разность имеет вид $\underbrace{1\ldots1}_{n}0\ldots0$. Поскольку 123456789 взаимно просто со степенями десяти, то $\underbrace{1\ldots1}_{n}$ кратно 123456789.

Комментарий

Мы использовали такое свойство делимости целых чисел:

$$ab \vdots c,\ b \text{ и } c \text{ взаимно просты } \Rightarrow a \vdots c.$$

Оно вытекает из однозначности разложения на простые множители (можно вывести также из алгоритма Евклида).

Так как $ab \vdots c$, то каждое простое p, входящее в разложение c в некоторой степени k, входит в разложение ab в степени $\geqslant k$. Но поскольку b и c взаимно просты, то у них нет общих простых делителей, поэтому p входит в разложение a в степени $\geqslant k$. Значит, $a \vdots c$.

Основная теорема арифметики

Каждое натуральное число раскладывается в произведение простых множителей, и притом однозначно.

(Напомним, что 1 не считается простым числом. Удобно считать, что 1 раскладывается в произведение нуля сомножителей.)
Так ли очевидна эта теорема? Существование разложения легко доказать по индукции. Но вот единственность – более тонкий факт.

Основная теорема арифметики

Лучший способ понять, что теорема не очевидна, — привести примеры, когда она ... неверна!

Мультипликативно замкнутые подмножества в $\mathbb{N}$

Пусть $M \subseteq \mathbb{N}$ — подмножество, в котором можно говорить о делимости. Для этого потребуем два свойства:
1) $1 \in M$;
2) если $a, b \in M$, то $ab \in M$ (M замкнуто относительно умножения).

Примеры

Какие из следующих подмножеств содержат 1 и замкнуты относительно умножения?

1) $2\mathbb{N}$ (чётные числа);

2) $2\mathbb{N} - 1$ (нечётные числа);

3) $4\mathbb{N}_0 + 1 = \{1, 5, 9, 13, \ldots\}$ (остаток 1 при делении на 4);

4) $2^{\mathbb{N}_0} = \{1, 2, 2^2, \ldots\}$ (степени двойки);

5) $\mathbb{N}^2 = \{1, 4, 9, 16, \ldots\}$ (квадраты).

Примеры

Пусть $M \subseteq \mathbb{N}$ содержит 1 и замкнуто относительно умножения. Пусть $a, b \in M$.

Определение. $a \vdots b$ в M значит, что $a = bc$ для некоторого $c \in M$.

Определение. Простые числа в M — это числа, имеющие в M ровно два делителя (себя и 1).

Упражнение. Опишите простые числа в следующих подмножествах:

1) $2\mathbb{N} - 1$ (нечётные числа);

2) $2^{\mathbb{N}_0} = \{1, 2, 2^2, \ldots\}$ (степени двойки);

3) $\mathbb{N}^2 = \{1, 4, 9, 16, \ldots\}$ (квадраты).

Верна ли в этих множествах основная теорема арифметики?

Множество загадочных степеней

Рассмотрим множество

$$M = \{1, 4, 8, 16, 32, \ldots\}$$

всех степеней двойки, кроме двойки (загадочность в том, что для описания M используется $2 \notin M$).

Верно ли, что в M: $8 \vdots 4$, $64 \vdots 16$, 4 — простое число?

Опишите простые числа в M.

Всякое число из M можно разложить на простые?

Всякое ли число из M однозначно раскладывается на простые?

Множество загадочных степеней: ответы

$8 \vdots 4$ в M — неверно, так как $8 = 4 \cdot 2$ в $\mathbb{N}$, причём частное 2 определено однозначно, но $2 \notin M$.
$64 \vdots 16$ в M — верно: $64 = 16 \cdot 4$ и $4 \in M$.
4 — простое число в M, так как 4 делится только на себя и 1 ($2 \notin M$).
Простые числа в M: 4 и 8 (остальные > 1 кратны 4).
Каждое число в M раскладывается на простые (индукция), но не всегда однозначно:

$$64 = 4 \cdot 4 \cdot 4 = 8 \cdot 8.$$

Прогрессия с загадочной разностью

Рассмотрим множество

$$M = \{1, 5, 9, 13, 17, \ldots\}$$

всех чисел, дающих остаток 1 при делении на 4 (загадочность в том, что для описания M используется $4 \notin M$).

Приведите примеры чисел, которые просты в M, но составные в $\mathbb{N}$.

Приведите пример неоднозначного разложения на простые в M.

Прогрессия с загадочной разностью

Число $9 = 3^2$ — составное в $\mathbb{N}$, но простое в M.
Другие примеры: $49 = 7^2$, $21 = 3 \cdot 7$ и т. п.
Вообще, все простые в M, которые раскладываются в $\mathbb{N}$, это произведения двух простых в $\mathbb{N}$, дающих остаток 3 при делении на 4.
Из них можно составить пример неоднозначного разложения:

$$3^2 \cdot 7^2 = (3 \cdot 7)^2.$$

$9, 49, 21$ — простые в M и $9 \cdot 49 = 21^2$.

План доказательства однозначности разложения в $\mathbb{N}$

Пусть $N = p_1 \dots p_n = q_1 \dots q_m$ — наименьшее число с неоднозначным разложением; все p_i и q_j — простые, причём можно считать, что $p_1 \neq q_1, \dots, q_m$.
Остаётся доказать **лемму**:

$$ab \vdots c,\ (b, c) = 1 \Rightarrow a \vdots c.$$

Применяя её последовательно, получим противоречие:
$q_1(q_2 \dots q_m) \vdots p_1,\ (p_1, q_1) = 1 \Rightarrow q_2 \dots q_m \vdots p_1$,
аналогично, $q_3 \dots q_m \vdots p_1$ и т. д. $q_m \vdots p_1$.

Лемма

$$ab \vdots c,\ (b,c) = 1 \Rightarrow a \vdots c.$$

Лемма доказывается с помощью обратного хода алгоритма Евклида, согласно которому

$$ub + vc = 1$$

для некоторых целых u и v. Умножим на a:

$$u \underbrace{ab}_{\vdots c} + vac = a \vdots c.$$

Задача

Сколько натуральных делителей у чисел:

а) 10^6;

б) 1001;

в) $11^{1001} \cdot 1001^{11}$?

Решение

а) $10^6 = 2^6 \cdot 5^6$. По основной теореме арифметики каждый делитель этого числа имеет вид $2^a 5^b$, где $0 \leqslant a, b \leqslant 6$. Каждый показатель a, b может принимать 7 значений $(0, 1, \ldots, 6)$, поэтому всего делителей у миллиона $7^2 = 49$.

б) Полезно помнить разложение

$$1001 = 7 \cdot 11 \cdot 13.$$

Каждый делитель имеет вид $7^a 11^b 13^c$, где $a, b, c \in \{0, 1\}$ — итого 2^3 делителей.

в) $11^{1001} \cdot 1001^{11} = 11^{1001} \cdot (7 \cdot 11 \cdot 13)^{11} = 7^{11} \cdot 11^{1012} \cdot 13^{11}$ — всего $(11 + 1)^2(1012 + 1)$ делителей.

Задача

Какие из следующих чисел простые?

$$6^{2020} - 1, \quad 2^{2020} - 1, \quad 2^{1001} - 1, \quad 2^7 - 1$$

Решение

Используем формулу

$$a^n - 1 = (a-1)(a^{n-1} + a^{n-2} + \ldots + a + 1).$$

Отсюда $a^n - 1 \vdots a - 1$ (более общо, $a^n - b^n \vdots a - b$).
Поэтому следующие числа составные:

$$6^{2020} - 1 \vdots 6 - 1,$$

$$2^{2020} - 1 = (2^{1010} - 1)(2^{1010} + 1),$$

$$2^{1001} - 1 = (2^{11})^{7 \cdot 13} - 1 \vdots 2^{11} - 1.$$

Числа Мерсенна

Вообще, если $n = ab$ составное $(1 < a, b < n)$, то $2^n - 1$ составное $(2^{ab} - 1 \vdots 2^a - 1)$. Вопрос — при каких простых p число $M_p = 2^p - 1$ — простое; M_p — **простые числа Мерсенна.**

При $p = 7$ имеем: $2^7 - 1 = 127$ не делится на $2, 3, 5, 7, 11$, а 13^2 уже больше 127, поэтому 127 — простое. Вообще, если N не делится ни на одной простое $\leqslant \sqrt{N}$, то N — простое, т. к. с каждым делителем k у числа n есть дополнительный делитель n/k. Значит, если есть делитель $k > \sqrt{N}$, то есть делитель $n/k < \sqrt{N}$.

Числа Мерсенна

Существует простое p, для которого $2^p - 1$ составное. Наименьшее такое $p = 11$:
$2^{11} - 1 = 2047 = 23 \cdot 89$.
Неизвестно, конечно или бесконечно множество простых чисел Мерсенна. В 2009 году с помощью компьютера было показано, что $2^{43112609} - 1$ — простое (приз — \$100000).
Числа Мерсенна используются в алгоритме проверки чисел на простоту (тест Люка–Лемера).

Задача

Пусть $2^n + 1$ — простое число. Докажите, что n — степень двойки.

Решение

Если n имеет нечётный делитель b, $n = ab$, то $2^{ab} + 1 = (2^a)^b + 1$ кратно $2^a + 1$, так как $x^b + 1 = x^b - (-1)^b$ кратно $x - (-1)$.
Поскольку $2^n + 1$ простое, то n не может иметь нечётных делителей, кроме 1. Это значит, что n — степень двойки.

Числа Ферма

Это числа вида $F_j = 2^{2^j} + 1$, где $j \in \mathbb{N}_0$. Первые 5 из них простые:

$$3, 5, 17, 257, 65537.$$

Ферма полагал, что они все простые, но Эйлер это опроверг, показав, что

$$F_5 = 2^{32} + 1 = 641 \cdot 6700417.$$

Есть ли ещё простые числа Ферма, неизвестно. Известно, что при $5 \leqslant j \leqslant 32$ они составные (есть и другие примеры составных чисел Ферма).

Теорема (частный случай теоремы Гаусса–Ванцеля). Правильный p-угольник, где p — простое, можно построить с помощью циркуля и линейки, если и только если p — простое число Ферма.

Задача

Найдите все $n \in \mathbb{N}$, при которых $n^4 + 4$ — простое число.

Решение

Теорема Софи Жермен. При всех $n > 1$ число $n^4 + 4$ — составное

$$n^4 + 4 = n^4 + 4 + 4n^2 - 4n^2 = (n^2 + 2)^2 - (2n)^2 =$$

$$= (\underbrace{n^2 - 2n + 2}_{(n-1)^2+1>1})(n^2 + 2n + 2).$$

При $n = 1$ получаем простое число $1^4 + 4 = 5$.

Теорема Евклида

Простых чисел бесконечно много.
От противного: пусть $p_1, \ldots, p_n$ — все простые числа. Рассмотрим число

$$M = p_1 \ldots p_n + 1.$$

У любого числа, большего 1, есть простой делитель — например, его наименьший делитель, больший 1. Но любой простой делитель числа M отличен от $p_1, \ldots, p_n$. Противоречие.

Задача

Докажите, что простых чисел вида
а) $3k-1$; б)* $3k+1$; в) $4k-1$; г)* $4k+1$
бесконечно много.

Решение а)

Предположим, что $p_1, \ldots, p_n$ — все простые числа вида $3k - 1$. Рассмотрим число

$$M = 3p_1 \ldots p_n - 1.$$

Все его простые делители отличны от 3 и от $p_1, \ldots, p_n$, а значит, все имеют вид $3k + 1$. Но тогда и само число M — произведение своих простых делителей — имеет тот же вид. Противоречие.

Теорема Дирихле

Любая арифметическая прогрессия $a, a + d, a + 2d, \ldots$, в которой a и d — взаимно простые натуральные числа, содержит бесконечно много простых чисел.