КИТАЙСКАЯ ТЕОРЕМА ОБ ОСТАТКАХ

П. В. Бибиков[1]

Содержание

1. Введение

Китайская теорема об остатках является незаслуженно забытой теоремой в курсе теории чисел. Обычно о ней говорят как о каком-то второстепенном результате, позволяющем строить остатки по большому модулю с помощью рассмотрения остатков по маленьким модулям (являющимся взаимно простыми делителями большого модуля). Подобный чисто вычислительный аспект обычно затмевает гораздо более важные идеи, связанные с применением китайской теоремы об остатках. Во-первых, эта теорема позволяет доказывать существование довольно сложных конструкций, используя простое соображение: системы линейных сравнений по взаимно простым модулям всегда существует решение. Во-вторых, эта теорема позволяет оценить это решение, что бывает полезно при каких-то численных оценках. Наконец, эта теорема позволяет хорошо взаимодействовать с делимостью, поскольку дает возможность рассматривать взаимно простые модули вместо большого составного.

Начнем с того, что приведем различные формулировки китайской теоремы б остатках и обсудим, как именно необходимо применять ее в задачах.

Теорема 1 (Китайская теорема об остатках)**.** *Для любых целых чисел $r_1, \ldots, r_n$ и любых попарно взаимно простых чисел $m_1, \ldots, m_n$ существует целое число x, такое, что $x \equiv r_i \pmod{m_i}$ для всех $i = 1, \ldots, n$. Более того, все такие числа сравнимы друг с другом по модулю $m_1 \ldots m_n$.*

Простейшая идеология применения китайской теоремы об остатках связана с рассмотрением вместо одного сложного сравнения нескольких простых. Главный вопрос, который обычно возникает, связан с тем, каким модули $m_1, \ldots, m_n$ нужно выбрать. Обычно это либо два соседних натуральных числа, либо степени простых, входящих в разложение некоторого числа на простые множители, либо различные простые числа, удовлетворяющие определенным условиям.

Посмотрим сначала на базовые задачи, связанные с применением китайской теоремы об остатках (КТО).

[1]Лицей «Вторая школа»; *e-mail*: bibikov.pv@sch2.ru

1. Пусть $p \neq q$ — простые числа. Найти остаток числа $p^q + q^p$ по модулю pq.

2. Докажите, что для каждого натурального n существуют такие натуральные a и b, что $n \mid 4a^2 + 9b^2 - 1$.

3. Докажите, что для каждого натурального n существует n последовательных натуральных чисел, не являющихся степенью простого числа.

4. Пусть n — натуральное число. Найдите количество таких натуральных $x \in \{1, 2, \ldots, n\}$, что $x^2 \equiv x \pmod{n}$.

2. Конструктивы

В этом разделе мы более подробно поговорим о способах применить китайскую теорему об остатках для доказательства существования чисел, удовлетворяющих тем или иным условиям. Отметим, что в теории чисел не так уж много теорем существования, позволяющих предъявлять те или иные объекты, не строя их явно, и китайская теорема об остатках, будучи очень естественным и интуитивно понятным результатом, без сомнения, является одной из самых главных таких теорем.

Еще раз отметим, что идеология применения китайской теоремы об остатках для построения числа (или чисел), обладающего каким-то сложным свойством, состоит в том, чтобы наложить *несколько простых* условий на это (пока неизвестное) число, из которых следует требуемое свойство. При этом условия могут быть более жесткими; главное, чтобы их можно было записать в виде *системы линейных сравнений*, разрешимость которой и гарантируется китайской теоремой об остатках.

5. Пусть p — простое число. Докажите, что существует бесконечно много натуральных n, таких, что $p | 2^n - n$.

6. Доказать, что для любого целого c и простого p существует такое целое x, что $x^x \equiv c \pmod{p}$.

7. Назовем целочисленную точку на координатной плоскости примитивной, если ее координаты взаимно просты. Докажите, что существует квадрат со стороной 2018, не содержащий примитивных точек.

8. Конечно ли множество чисел вида $2^n - 1$, у которых больше миллиона различных простых делителей?

9. Докажите, что существует бесконечно много попарно взаимно простых чисел виде $2^n - 3$.

10. Доказать, что для любой последовательности натуральных чисел $\{a_1, \ldots, a_n\}$ найдется такое натуральное b, что $\{ba_1, \ldots, ba_n\}$ — точные степени, большие 1 (т.е. $ba_i = x_i^{m_i}$, где $m_i > 1$).

11. Докажите, что для любого натурального n существуют попарно взаимно простые натуральные числа k_1, …, k_n, большие 1, такие, что число $k_1 \ldots k_n - 1$ равно произведению двух последовательных натуральных чисел.

12. Докажите, что существует бесконечная монотонно возрастающая последовательность натуральных чисел $\{a_n\}$, такая, что при всех целых $k \geqslant 0$ последовательность $\{k + a_n\}$ содержит лишь конечное число простых чисел.

3. Делимость и остатки

Цель этого раздела — научиться использовать китайскую теорему об остатках для решения задач,связанных с делимостью. Как правило, здесь требуются т же самые идеи, что и при решении задач на конструктивы. Особенно отметим идею выделять в натуральных числах простые сомножители (или их степени), и изучать делимость для каждого сомножителя по отдельности.

13. Пусть n — натуральное число и $a_1, \ldots, a_k$ — различные числа из множества $\{1, 2, \ldots, n\}$ (здесь $2 \leqslant k \leqslant n$), такие, что $n \mid a_i(a_{i+1} - 1)$ для всех $i = 1, 2, \ldots, k-1$. Докажите, что $n \nmid a_k(a_i + 1)$.

14. Пусть $a > b > c \geqslant 3$ — натуральные числа, такие, что $a \mid bc+b+c$, $b \mid ca+c+a$, $c \mid ab+a+b$. Докажите, что хотя бы одно из чисел a, b, c составное.

15. Докажите, что для каждого натурального n существует такое множество S из n натуральных чисел, что для любых двух чисел a, $b \in S$ разность $a - b$ делит a и b, но не делит ни одно другое число из S.

16. Для каждого конечного множества X определим числа $S(X) = \sum\limits_{x \in X} x$ и $P(X) = \prod\limits_{x \in X} x$. Пусть A и B — два конечных множества, таких, что $P(A) = P(B)$, $S(A) \neq S(B)$ и для каждого $n \in A \cup B$ любое простое число, входящее в его разложение, входит в точности в степени 36. Доказать, что $|S(A) - S(B)| > 1{,}9 \cdot 10^6$.

17. Найти все тройки натуральных чисел $(a; b; c)$, для которых выполнено следующее условие: если n — натуральное число, не имеющее простых делителей, меньших 2019, то $n+c \mid a^n+b^n+n$.

18. Пусть $f\colon \mathbb{N} \to \mathbb{N}$ — такая функция, что
1) если $(m, n) = 1$, то $(f(m), f(n)) = 1$;
2) $n \leqslant f(n) \leqslant n + 2019$ для всех n.
Докажите, что если простое число p делит число $f(n)$, то $p \mid n$.

19. Найти все многочлены $P \in \mathbb{Z}[x]$, такие, что на целочисленной прямой $\mathbb{Z}$ можно так расставить все натуральные числа, чтобы сумма чисел, стоящих внутри произвольного отрезка длины n, делится на $P(n)$.

4. Разные задачи

20. Генерал хочет построить для парада своих солдат в одинаковые квадратные каре (в каре должно быть больше одного человека), но он не знает сколько солдат (от 1 до 42) находится в лазарете. Докажите, что у генерала может быть такое количество солдат, что он, независимо от заполнения лазарета, сумеет выполнить свое намерение. (Например, войско из 9 человек можно поставить в виде квадрата 3×3, а если один человек болен, то в виде двух квадратов 2×2.)

21. Про многочлен $p(x)$ с целыми коэффициентами известно, что для любого целого n число $p(n)$ делится на одно из целых чисел $a_1, \ldots, a_m$. Докажите, что из этих чисел можно выбрать одно число так, что $p(n)$ будет делиться на него при любом целом n.

22. Докажите, что для любого натурального n существует такое множество из n натуральных чисел, что всевозможные суммы элементов этого множества являются степенями натуральных

чисел (степени должны быть больше 1).

23. Докажите, что для любого натурального n существует арифметическая прогрессия длины n, состоящая из точных степеней натуральных чисел (каждая степень должна быть больше 1).

24. Докажите, что для каждого натурального k существует арифметическая прогрессия, состоящая из несократимых рациональных дробей, все числители из знаменатели которых попарно различны.

25. При каких натуральных $n > 1$ существуют такие натуральные $b_1, \ldots, b_n$ (не все из которых равны), что при всех натуральных k число $(b_1 + k)(b_2 + k)\ldots(b_n + k)$ является степенью натурального числа? (Показатель степени может зависеть от k, но должен быть больше 1.)

26. Пусть $m_1, \ldots, m_{2019} > 1$ — попарно взаимно простые натуральные числа и $A_1, \ldots, A_{2019}$ — множества (возможно пустые), такие, что $A_i \subseteq \{1, 2, \ldots, m_i - 1\}$. Докажите, что существует такое натуральное N, что

$$N \leqslant (2|A_1| + 1)(2|A_2| + 1)\ldots(2|A_{2019}| + 1)$$

и $N \notin A_i \pmod{m_i}$.

27. Докажите, что существует константа $c > 0$, обладающая следующим свойством. Если a, b, n — натуральные числа, такие, что $(a + i, b + j) > 1$ для всех $i, j \in \{0, 1, \ldots, n\}$, то $a, b > (cn)^n$.

5. Решения задач

5.1. Введение

1. Пусть $p \neq q$ — простые числа. Найти остаток числа $p^q + q^p$ по модулю pq.

Решение. Пусть $x \equiv p^q + q^p \pmod{pq}$ — искомый остаток. Согласно КТО, достаточно найти решение сравнений $x \equiv p^q + q^p \pmod{p, q}$. Но

$$x \equiv p^q + q^p \equiv q^p \equiv q \pmod{p} \quad \text{и} \quad x \equiv p^q + q^p \equiv p^q \equiv p \pmod{q}.$$

Легко видеть, что $x = p + q$ удовлетворяет обоим сравнениям, и $p + q < p^q + q^p$. Значит, это и есть искомый остаток.

Ответ: $p + q$.

2. Докажите, что для каждого натурального n существуют такие натуральные a и b, что $n \mid 4a^2 + 9b^2 - 1$.

Решение. Согласно КТО, достаточно доказать существование таких a и b для $n = p^k$ — степени простого числа. Если $n = 2^k$, положим $a \equiv 0 \pmod{2^k}$ и $b \equiv 3^{-1} \pmod{2^k}$. Для $p > 2$ положим $a \equiv 2^{-1} \pmod{p^k}$ и $b \equiv 0 \pmod{p^k}$.

3. Докажите, что для каждого натурального n существует n последовательных натуральных чисел, не являющихся степенью простого числа.

Решение. Мы предъявим последовательность из n последовательных натуральных чисел, каждое из которых содержит хотя бы два простых делителя. Для этого выберем $2n$ различных простых чисел $p_1, q_1, p_2, q_2, \ldots, p_n, q_n$ и рассмотрим систему сравнений $x \equiv -i \pmod{p_i q_i}$. По КТО у этой системы существует решение x_0. Тогда числа $x_0 + 1, x_0 + 2, \ldots, x_0 + n$ — искомые.

4. Пусть n — натуральное число. Найдите количество таких натуральных $x \in \{1, 2, \ldots, n\}$, что $x^2 \equiv x \pmod{n}$.

Решение. Пусть $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ — разложение числа n на простые. Согласно КТО, если $x_i^2 \equiv x_i \pmod{p_i^{\alpha_i}}$, то $x = x_1 \dots x_k$ удовлетворяет сравнению $x^2 \equiv x \pmod{n}$. Но $x_i(x_i - 1) \equiv 0 \pmod{p_i^{\alpha_i}}$ возможно лишь в двух случаях: $x_i \equiv 0 \pmod{p_i^{\alpha_i}}$ и $x_i \equiv 1 \pmod{p_i^{\alpha_i}}$. Значит, для каждого i существует лишь два решения сравнения $x_i^2 \equiv x_i \pmod{p_i^{\alpha_i}}$. Таким образом, количество способов выбрать из каждого такого сравнения одно решение равно 2, а количество всевозможных произведений равно 2^k.

Ответ: 2^k, где k — количество простых множителей в разложении числа n на простые.

5.2. Конструктивы

5. Пусть p — простое число. Докажите, что существует бесконечно много натуральных n, таких, что $p|2^n - n$.

Решение. Рассмотрим систему линейных сравнений $n \equiv 0 \pmod{p-1}$, $n \equiv 1 \pmod{p}$. Согласно КТО, у этой системы существует бесконечно много натуральных решений. Из малой теоремы Ферма следует, что все они удовлетворяют условию.

6. Доказать, что для любого целого c и простого p существует такое целое x, что $x^x \equiv c \pmod{p}$.

Решение. Рассмотрим систему линейных сравнений $x \equiv 0 \pmod{p-1}$, $x \equiv c \pmod{p}$. Согласно КТО, у этой системы существует бесконечно много натуральных решений. Из малой теоремы Ферма следует, что все они удовлетворяют условию.

7. Назовем целочисленную точку на координатной плоскости примитивной, если ее координаты взаимно просты. Докажите, что существует квадрат со стороной 2018, не содержащий примитивных точек.

Решение. Рассмотрим n^2 различных простых чисел p_{ij}, где $n = 2018$ и $i, j = 1, \dots, n$. Пусть $(x; y)$ — целочисленная точка. рассмотрим систему сравнений $x \equiv -i \pmod{p_{ij}}$, $y \equiv -j \pmod{p_{ij}}$ для всех $i, j = 1, \dots, n$. Согласно КТО, у этой системы существует натуральное решение $(x_0; y_0)$. Тогда квадрат с вершиной $(x_0 + 1; y_0 + 1)$ — искомый, т.к. $p_{ij} \mid x_0 + i$ и $p_{ij} \mid y_0 + j$.

8. Конечно ли множество чисел вида $2^n - 1$, у которых больше миллиона различных простых делителей?

Решение. Докажем, что таких натуральных чисел бесконечно много. Рассмотрим миллион простых делителей $p_1, p_2, \dots$ и возьмем $n = k(p_1-1)(p_2-1)\dots$, где k — произвольное натуральное число. Согласно малой теореме Ферма, все такие n подходят.

9. Докажите, что существует бесконечно много попарно взаимно простых чисел виде $2^n - 3$.

Решение. Пусть мы построили набор попарно взаимно простых чисел $2^{n_1} - 3$, $2^{n_2} - 3$, …, $2^{n_k} - 3$. Рассмотрим все простые делители p_1, p_2, …этих чисел. Ясно, что все эти простые делители нечетны. Возьмем число $n_{k+1} = (p_1 - 1)(p_2 - 1)\dots$. Если бы $p_i \mid 2^{n_{k+1}} - 3$, то согласно малой теореме Ферма $2^{n_{k+1}} - 3 \equiv 1 - 3 = -2 \not\equiv 0 \pmod{p_i}$, т.к. p_i нечетно. Значит, число $2^{n_{k+1}} - 3$ взаимно просто со всеми уже выписанными числами $2^{n_1} - 3$, $2^{n_2} - 3$, …, $2^{n_k} - 3$. Продолжая этот процесс, получаем бесконечное множество искомых чисел.

10. Доказать, что для любой последовательности натуральных чисел $\{a_1, \dots, a_n\}$ найдется такое натуральное b, что $\{ba_1, \dots, ba_n\}$ — точные степени, большие 1 (т.е. $ba_i = x_i^{m_i}$, где $m_i > 1$).

Решение. Пусть p_1, …, p_k — все простые делители чисел a_1, …, a_n. Пусть $a_i = p_1^{\alpha_{i1}} \dots p_k^{\alpha_{ik}}$, где $\alpha_{ij} \geqslant 0$. Будем искать число b в виде $p_1^{\beta_1} \dots p_k^{\beta_k}$. Тогда условие $ba_i = x_i^{m_i}$ переписывается в

виде $\beta_j + \alpha_{ij} \equiv 0 \pmod{m_i}$. Выберем взаимно простые числа $m_1, \ldots, m_n$ и применим КТО. В результате мы получим набор степеней $\beta_1, \ldots, \beta_k$ и искомое число $b = p_1^{\beta_1} \ldots p_k^{\beta_k}$.

11. Докажите, что для любого натурального n существуют попарно взаимно простые натуральные числа $k_1, \ldots, k_n$, большие 1, такие, что число $k_1 \ldots k_n - 1$ равно произведению двух последовательных натуральных чисел.

Решение. Пусть $P(x) = x^2 + x + 1$. Сначала докажем, что количество простых делителей чисел вида $x^2 + x + 1$ бесконечно. В самом деле, предположим, что существует лишь конечное число простых делителей у чисел вида $x^2 + x + 1$. Выпишем все такие делители, обозначим через N их произведение и рассмотрим число $P(N) = N^2 + N + 1$. Его простой делитель отличен от предыдущих и делит $P(N)$ — противоречие.

Итак, существует бесконечно много простых делителей чисел вида $P(x) = x^2 + x + 1$. Зафиксируем n простых чисел $p_1, \ldots, p_n$, являющихся делителями чисел вида $P(x)$, и рассмотрим такие x_i, что $P(x_i) \equiv 0 \pmod{p_i}$. Положим $y \equiv x_i \pmod{p_i}$. По КТО такой y существует. Тогда $P(y) \equiv P(x_i) \equiv 0 \pmod{p_i}$. Значит, у числа $P(y)$ есть хотя бы n простых делителей. Но тогда число $x^2 + x + 1$ представимо в виде произведения n попарно взаимно простых чисел, что и требовалось доказать.

12. Докажите, что существует бесконечная монотонно возрастающая последовательность натуральных чисел $\{a_n\}$, такая, что при всех целых $k \geqslant 0$ последовательность $\{k + a_n\}$ содержит лишь конечное число простых чисел.

Решение. Пусть p_k — k-е простое число. Положим $a_1 = 2$. Для $n \geqslant 1$ определим a_{n+1} как наименьшее натуральное число, большее a_n и сравнимое с $-k \pmod{p_{k+1}}$ для всех $k \leqslant n$. Согласно КТО такое число существует. Тогда $k + a_n \equiv 0 \pmod{p_{k+1}}$ для всех $n \geqslant k + 1$. Таким образом, не более $k + 1$ элементов последовательности $\{k + a_n\}$ являются простыми числами.

5.3. Делимость и остатки

13. Пусть n — натуральное число и $a_1, \ldots, a_k$ — различные числа из множества $\{1, 2, \ldots, n\}$ (здесь $2 \leqslant k \leqslant n$), такие, что $n \mid a_i(a_{i+1} - 1)$ для всех $i = 1, 2, \ldots, k - 1$. Докажите, что $n \nmid a_k(a_i + 1)$.

Решение. Предположим противное: пусть $n \mid a_i(a_{i+1} - 1)$ для всех $i = 1, 2, \ldots, k$ (мы считаем, что $a_{k+1} = a_1$). Пусть $p \mid n$ — какой-то простой делитель n, входящий в его разложение на простые сомножители в степени r. Тогда $p \mid a_i(a_{i+1} - 1)$ для всех i. Предположим, что $p \mid a_i$ для некоторого i. Тогда $p \nmid a_i - 1$, а потому $p \mid a_{i-1}$. Рассуждая аналогично, получаем, что $p \mid a_i$ для всех i. Значит, либо $a_i \equiv 0 \pmod{p}$, либо $a_i \equiv 1 \pmod{p}$. Более того, либо $a_i \equiv 0 \pmod{p^r}$, либо $a_i \equiv 1 \pmod{p^r}$. Проводя это рассуждение для каждого простого делителя числа n, получаем, что все эти простые делители разбиваются на две группы: в первой они делят все a_i, а во второй — все $a_i - 1$. Обозначим их произведения через x и y. Но тогда $a_i \equiv 0 \pmod{x}$ и $a_i \equiv 1 \pmod{y}$. Согласно КТО, у этой системы сравнений существует единственное решение по модулю $xy = n$. Но тогда все a_i совпадают — противоречие.

14. Пусть $a > b > c \geqslant 3$ — натуральные числа, такие, что $a \mid bc + b + c$, $b \mid ca + c + a$, $c \mid ab + a + b$. Докажите, что хотя бы одно из чисел a, b, c составное.

Решение. Предположим противное: пусть a, b и c простые. Перепишем условие в виде

$$\begin{cases}(a+1)(b+1)(c+1) \equiv 1 \pmod a\\(a+1)(b+1)(c+1) \equiv 1 \pmod b\\(a+1)(b+1)(c+1) \equiv 1 \pmod c.\end{cases}$$

Тогда по КТО $1 \equiv (a+1)(b+1)(c+1) \equiv ab+bc+ca+a+b+c+1 \pmod{abc}$. Но заметим, что $0 < ab+bc+ca+a+b+c < abc$, т.к.

$$\frac{1}{a}+\frac{1}{b}+\frac{1}{c}+\frac{1}{ab}+\frac{1}{bc}+\frac{1}{ca} < \frac{1}{3}+\frac{1}{5}+\frac{1}{7}+\frac{1}{15}+\frac{1}{21}+\frac{1}{35} < 1$$

— противоречие.

15. Докажите, что для каждого натурального n существует такое множество S из n натуральных чисел, что для любых двух чисел a, $b \in S$ разность $a-b$ делит a и b, но не делит ни одно другое число из S.

Решение. Пусть $d_1, \ldots, d_{n-1}$ — последовательность разностей между соседними элементами из S, упорядоченными по возрастанию. Положим также $s_k = d_1 + \ldots + d_{k-1}$ и $t_{ij} = d_i + \ldots + d_j$ (где $i \leqslant j$). Мы хотим построить последовательность $d_1, \ldots, d_{n-1}$ так, чтобы были выполнены следующие условия:

- никакие два числа вида t_{ij} н делят друг друга;
- существует такое натуральное a, что $a \equiv -s_i \pmod{t_{ij}}$ для всех $i \leqslant j$.

В этом случае последовательность $a+s_1, \ldots, a+s_n$ подходит. Будем строить последовательность $d_1, \ldots, d_{n-1}$ по индукции. База $d_1 = 2$, $d_2 = 3$. Покажем, как построить последовательность из n чисел. Для этого рассмотрим число $M = d_1 \ldots d_{n-1}$ и простое число $p \nmid M$. Докажем, что последовательность $d_1M, \ldots, d_{n-1}M, p$ подходит. В самом деле, первое условие очевидно, а второе следует из КТО: достаточно взять решение системы сравнений $a \equiv -s_i \pmod{t_{ij}}$ для всех $i \leqslant j$, $a \equiv 0 \pmod M$, $a \equiv -s_n \pmod p$.

16. Для каждого конечного множества X определим числа $S(X) = \sum\limits_{x\in X} x$ и $P(X) = \prod\limits_{x\in X} x$. Пусть A и B — два конечных множества, таких, что $P(A) = P(B)$, $S(A) \neq S(B)$ и для каждого $n \in A \cup B$ любое простое число, входящее в его разложение, входит в точности в степени 36. Доказать, что $|S(A) - S(B)| > 1{,}9 \cdot 10^6$.

Решение. Пусть p — такое простое число, что $p-1 \mid 36$. Тогда согласно малой теореме Ферма для любого элемента $a \in A$ либо $a \equiv 1 \pmod p$, либо $a \equiv 0 \pmod p$. Заметим, что количество чисел из множества A, которые кратны p, равно количеству чисел из множества B, которые кратны p. Поэтому равны и количества чисел, сравнимых с 1 по модулю p. Значит, $p \mid S(A) - S(B)$ и $2{\cdot}3{\cdot}5{\cdot}7{\cdot}13{\cdot}19{\cdot}37 \mid |S(A)-S(B)|$, и т.к. $S(A) \neq S(B)$, то $|S(A)-S(B)| \geqslant 2{\cdot}3{\cdot}5{\cdot}7{\cdot}13{\cdot}19{\cdot}37 = 1919190$, что и требовалось доказать.

17. Найти все тройки натуральных чисел $(a; b; c)$, для которых выполнено следующее условие: если n — натуральное число, не имеющее простых делителей, меньших 2019, то $n+c \mid a^n+b^n+n$.

Решение. Пусть $q_1, \ldots, q_k$ — первые k простых чисел, среди которых есть все простые числа, меньшие 2019. Пусть p — простой делитель числа $q_1 \ldots q_k + 1$, больший a^2, b^2 и c (этого всегда можно добиться, взяв достаточно большое k). Рассмотрим натуральное число n, такое, что $n \equiv -c \pmod p$ и $n \equiv 1 \pmod{p-1}$ (по КТО такое число существует). Тогда $p \mid n+c \mid a^n+b^n+n$, откуда

$$0 \equiv a^n + b^n + n \equiv a + b - c \pmod p.$$

Таким образом, $a+b \equiv c \pmod p$. Значит, $a+b=c$ (т.к. a, b, $c<p$). Теперь рассмотрим такое n, что $n \equiv -c \pmod p$ и $n \equiv 2 \pmod{p-1}$. Проводя аналогичные рассуждения, получим, что $a^2+b^2=c$. Значит, $a=b=1$ и $c=2$.

Ответ: $(1;1;2)$.

18. Пусть $f\colon \mathbb{N} \to \mathbb{N}$ — такая функция, что

1) если $(m,n)=1$, то $(f(m),f(n))=1$;

2) $n \leqslant f(n) \leqslant n+2019$ для всех n.

Докажите, что если простое число p делит число $f(n)$, то $p \mid n$.

Решение. Предположим, что нашлись такие n и p, что p простое, $p \mid f(n)$ и $p \nmid n$. Построим такое натуральное N, что $f(N)=N$. Для этого зафиксируем $2019 \cdot 2020$ различных простых чисел $q_{ij} > n+p+2020$ (здесь $i=1,\ldots,2019$ и $j=0,\ldots,2019$) и рассмотрим следующую таблицу:

	$N+1$	$N+2$	$\ldots$	$N+2019$
M	q_{01}	q_{02}	$\ldots$	$q_{0;2019}$
$M+1$	q_{11}	q_{12}	$\ldots$	$q_{1;2019}$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
$M+2019$	$q_{2019,;1}$	$q_{2019;2}$	$\ldots$	$q_{2019;2019}$

Согласно КТО, существует такое натуральное N, что $N+j \equiv 0 \pmod{q_{ij}}$, $N \equiv 0 \pmod p$ и $N \equiv 1 \pmod n$, где $j=1,\ldots,2019$. Ясно, что $q_{ij} \nmid N$.

Теперь выберем такое M, что $M+i \equiv 0 \pmod{q_{ij}}$ и $M \equiv 1 \pmod N$. Согласно КТО, такое число M существует.

Заметим, что $(M,N)=1$, поэтому $(f(M),f(N))=1$. Но число $f(M)$ равно $M+i$, а значит, оно не взаимно просто с некоторым числом $N+j$, т.к. оба они делятся на q_{ij}. Значит, $f(N) \neq N+i$ для $i>0$, а потому $f(N)=N$.

Наконец, $(n,N)=1$, а потому $(f(n),N)=(f(n),f(N))=1$. Но $p \mid N$ и $p \mid f(n)$ — противоречие.

19. Найти все многочлены $P \in \mathbb{Z}[x]$, такие, что на целочисленной прямой $\mathbb{Z}$ можно так расставить все натуральные числа, чтобы сумма чисел, стоящих внутри произвольного отрезка длины n, делится на $P(n)$.

Решение. Пусть на i-м месте стоит число $g(i)$. Тогда из условий $P(n) \mid g(i)+\ldots+g(i+n-1)$, $g(i+1)+\ldots+g(i+n)$ следует, что $P(n) \mid g(i)-g(i+n)$. Аналогично, $P(m) \mid g(i)-g(i+m)$. Поэтому по алгоритму Евклида мы получаем, что $(P(n),P(m)) \mid g(i)-g(i+(n,m))$.

Выберем теперь взаимно простые m и n и $i=0$. Докажем, что НОД $(P(n),P(m))$ может быть сколь угодно велик, если только $P(x) \neq cx^k$. Действительно, пусть $P(x)=x^kQ(x)$, и $Q \neq \text{const}$. Тогда существует бесконечно много простых чисел, делящих числа вида $Q(n)$ (доказательство этого утверждения аналогично рассуждению из задачи 11). Зафиксируем такое простое число $p > q(0)-g(1)$, которое не делит $Q(0)$, и рассмотрим попарно взаимно простые числа m, n такие, что $p \mid Q(m)$, $Q(n)$ (например, можно взять $n=m+p$: т.к. $p \nmid Q(0)$, то $p \nmid m$). Тогда $p \leqslant (Q(m),Q(n)) \leqslant (P(m),P(n)) \mid g(0)-g(1) < p$ — противоречие.

Осталось показать, что для $P(x)=cx^k$ требуемая расстановка существует. Для этого начнем заполнять прямую $\mathbb{Z}$ с числа $P(1)$, поставленного в точку 0, а затем будем поочередно ставить числа $g(1)$, $g(-1)$, $g(2)$, $g(-2)$, $\ldots$, используя условия $P(n) \mid g(i)+\ldots+g(i+n-1)$. По КТО получаем требуемую конструкцию.

5.4. Разные задачи

20. Генерал хочет построить для парада своих солдат в одинаковые квадратные каре (в каре должно быть больше одного человека), но он не знает сколько солдат (от 1 до 42) находится в лазарете. Докажите, что у генерала может быть такое количество солдат, что он, независимо от заполнения лазарета, сумеет выполнить свое намерение. (Например, войско из 9 человек можно поставить в виде квадрата 3×3, а если один человек болен, то в виде двух квадратов 2×2.)

Решение. Пусть $p_1, \ldots, p_{42}$ — различные простые числа. Согласно КТО, существует такое натуральное n, что $n \equiv i \pmod{p_i^2}$. Тогда, если у генерала в лазарете находятся i солдат, то оставшиеся $x - i$ солдаты могут быть разбиты на каре размера $p_i \times p_i$.

21. Про многочлен $p(x)$ с целыми коэффициентами известно, что для любого целого n число $p(n)$ делится на одно из целых чисел $a_1, \ldots, a_m$. Докажите, что из этих чисел можно выбрать одно число так, что $p(n)$ будет делиться на него при любом целом n.

Решение. Предположим противное: пусть для каждого i найдется такое n_i, что $a_i \nmid p(n_i)$. Тогда найдется такая степень простого $p_i^{\alpha_i}$, на которую не делится $p(n_i)$. Выберем такие степени простых для каждого i и если простые p_i будут совпадать, оставим одно p_iс наименьшей степенью. В результате мы получим набор степеней $p_i^{\alpha_i}$. По КТО существует такое натуральное n, что $n \equiv n_i \pmod{p_i^{\alpha_i}}$. Заметим, что $p(n) \equiv p(n_i) \not\equiv 0 \pmod{p_i^{\alpha_i}}$ для всех i, а значит, $p(n)$ не делится ни на одно из чисел $a_1, \ldots, a_m$ — противоречие.

22. Докажите, что для любого натурального n существует такое множество из n натуральных чисел, что всевозможные суммы элементов этого множества являются степенями натуральных чисел (степени должны быть больше 1).

Решение. Рассмотрим произвольное множество из элементов $\{a_1, \ldots, a_n\}$. Обозначим через S_1, $\ldots$, S_r всевозможные суммы его элементов. Согласно задаче **10** найдется такое натуральное b, что $bS_1, \ldots, bS_r$ — точные степени натуральных. Тогда множество $\{ba_1, \ldots, ba_n\}$ удовлетворяет условию задачи.

23. Докажите, что для любого натурального n существует арифметическая прогрессия длины n, состоящая из точных степеней натуральных чисел (каждая степень должна быть больше 1).

Решение. Рассмотрим произвольную арифметическую прогрессию $\{a_1, \ldots, a_n\}$. Согласно задаче **10** найдется такое натуральное b, что $ba_1, \ldots, ba_n$ — точные степени натуральных. Тогда прогрессия $\{ba_1, \ldots, ba_n\}$ удовлетворяет условию задачи.

24. Докажите, что для каждого натурального k существует арифметическая прогрессия, состоящая из несократимых рациональных дробей, все числители из знаменатели которых попарно различны.

Решение. Зафиксируем $2k$ различных простых чисел $p_1, \ldots, p_k, q_1, \ldots, q_k$, каждое из которых больше k. Положим $N = p_1 \ldots p_k$. Заметим, что числа

$$\frac{x+1}{N}, \quad \frac{x+2}{N} \quad \ldots \frac{x+k}{N}$$

образуют арифметическую прогрессию. Выберем x таким образом, чтобы i-я дробь сократилась в точности на число p_i, а числители делились бы на q_i. Для этого запишем следующую систему сравнений: $x+i \equiv 0 \pmod{p_i q_i}$. Заметим, что тогда ни одна другая дробь не сокращается на $p_i q_i$, т.к. иначе $0 \equiv x + j \equiv j - i \pmod{p_i, q_i}$, откуда $i \equiv j \pmod{p_i, q_i}$ и $i = j$ (т.к. $|i - j| < k < p_i, q_i$).

Значит, все числители и все знаменатели попарно различны, т.к. у них разные наборы простых делителей.

25. При каких натуральных $n > 1$ существуют такие натуральные $b_1, \ldots, b_n$ (не все из которых равны), что при всех натуральных k число $(b_1 + k)(b_2 + k)\ldots(b_n + k)$ является степенью натурального числа? (Показатель степени может зависеть от k, но должен быть больше 1.)

Решение. Пусть n — составное число, то есть $n = rs$, где $r, s > 1$. Тогда достаточно рассмотреть числа $b_1 = \ldots = b_r = 1$, $b_{r+1} = \ldots = b_n = 2$. Очевидно, что при всяком k число $(b_1+k)\ldots(b_n+k)$ является r-й степенью натурального числа.

Пусть теперь n — простое число и существует требуемый набор $(b_1, \ldots, b_n)$. Без ограничения общности можно считать, что $b_1, \ldots, b_q$ — попарно различные числа, а каждое из чисел $b_{q+1}, \ldots, b_n$ равно одному из $b_1, \ldots, b_q$ (здесь $q > 1$, так как не все числа равны). Пусть среди чисел $b_1, \ldots, b_n$ имеется s_i чисел, равных b_i, где $1 \leqslant i < q$, $s_1 + \ldots + s_q = n$.

Рассмотрим q различных простых чисел $p_1, \ldots, p_q$, которые больше всех b_i. Числа p_i^2 попарно взаимно просты и $0 < r_i < p_i < p_i^2$. По КТО найдчтся такое целое m, что $m \equiv p_i - b_i \pmod{p_i^2}$ при всех i от 1 до q. Пусть $(b_1 + m)\ldots(b_n + m) = u^v$.

Заметим, что $b_i + m \equiv p_i \pmod{p_i^2}$ т.е. число $b_i + m$ делится на p_i и не делится на p_i^2. При $j \neq i$, $1 \leqslant j \leqslant q$ имеем $0 < |b_i b_j| < p_i$, поэтому $b_j + m$ на p_i не делится.

Таким образом, в каноническом разложении числа $(b_1+m)\ldots(b_n+m)$ на простые множители каждое число p_i содержится ровно в степени s_i. Значит, число v является делителем всех s_i, а значит, и делителем их суммы n. При этом $v < n$, поэтому $v = 1$.

26. Пусть $m_1, \ldots, m_{2019} > 1$ — попарно взаимно простые натуральные числа и $A_1, \ldots, A_{2019}$ — множества (возможно пустые), такие, что $A_i \subseteq \{1, 2, \ldots, m_i - 1\}$. Докажите, что существует такое натуральное N, что

$$N \leqslant (2|A_1| + 1)(2|A_2| + 1)\ldots(2|A_{2019}| + 1)$$

и $N \notin A_i \pmod{m_i}$.

Решение. По сути необходимо доказать, что первое натуральное число, не покрытое множествами $A_i \pmod{m_i}$, не превосходит указанной в формулировке задачи величины. Для этого соединим КТО и интерполяционный многочлен Лагранжа следующим образом. Для каждого множества A_i рассмотрим множество B_i, состоящее из всех тех чисел A_i, чья разность не лежит в A_i. Заметим, что множества B_i содержат 0 и потому непусты.

Докажем, что $|B_i| \geqslant \dfrac{m_i}{2|A_i| + 1}$. Ясно, что любое число $x \pmod{m_i}$ лежит в одном из множеств B_i, $B_i + A_i$, $B_i - A_i$. Следовательно,

$$m_i \leqslant |B_i| + |B_i + A_i| + |B_i - A_i| \leqslant |B_i|(1 + 2|A_1|).$$

Теперь рассмотрим числа t_i, такие, что $t_i \equiv 1 \pmod{m_i}$ и $t_i \equiv 0 \pmod{m_j}$ для $j \neq i$. Линейные комбинации $b_1 t_1 + \ldots + b_{2019} t_{2019} \pmod{m_1 \ldots m_{2019}}$ являются различными в силу КТО, а значит, по принципу Дирихле найдутся две такие комбинации, отличающиеся не более чем на

$$N \leqslant \frac{m_1 m_2 \ldots m_{2019}}{|B_1||B_2|\ldots|B_{2019}|} \leqslant (2|A_1| + 1)(2|A_2| + 1)\ldots(2|A_{2019} + 1|),$$

что и требовалось доказать.

Замечание 1. На самом деле можно усилить оценку на N:

$$N \leqslant (|A_1| + 1)(|A_2| + 1)\ldots(|A_{2019}| + 1).$$

Предположим, что все числа от 1 до N покрываются множествами $A_i \pmod{m_i}$. Тогда число

$$z_n = \prod_{k;a\in A_k} \left(1 - e^{\frac{2\pi i}{m_k}(n-a)}\right)$$

является элементом линейной рекуррентности чисел $e^{2\pi i \sum \frac{j_k}{m_k}}$, где $j_k = 0, 1, \ldots, |A_k|$. Но $z_0 \neq 0 = z_1 = \ldots = z_N$, поэтому N строго меньше степени $\prod(|A_i|+1)$ этой линейной рекуррентности. Следовательно, все числа от 1 до $\prod(|A_i|+1)$ не могут быть покрыты, что и требовалось доказать.

Замечание 2. Из этой задачи можно получить следующее красиво следствие. Пусть f — целозначный многочлен, причем НОД его значений в целых точках в совокупности равен 1. Тогда существует бесконечно много натуральных n, таких, что наименьший простой делитель числа $f(n)$ не меньше $c \ln n$ для произвольной константы c. В самом деле, рассмотрим числа m_i, являющиеся занумерованными по порядку простыми числами и множества $A_i = \{n : m_i \mid f(n)\} \pmod{m_i}$. Тогда $|A_i| \leqslant \deg = d$ для достаточно больших n.

27. Докажите, что существует константа $c > 0$, обладающая следующим свойством. Если a, b, n — натуральные числа, такие, что $(a+i, b+j) > 1$ для всех i, $j \in \{0, 1, \ldots, n\}$, то a, $b > (cn)^n$.

Решение. Выпишем таблицу $N \times N$, где $N = n + 1$ и на (i, j)-м месте стоит простое число p_{ij}, делящее $a + i$ и $b + j$ (если таких простых чисел несколько, выберем любое и них). Пусть $M = 0{,}001n^2$. Заметим, что доля каждого из простых чисел p занимает в таблице не более p^{-2} части клеток. Оценим общее количество клеток в таблице, которые покрыты простыми числами, не превосходящими M. Пусть этих чисел r штук. Тогда $r < M < 0{,}001N^2$ и покрытых клеток не больше, чем

$$\sum_p \left\lceil \frac{N}{p} \right\rceil^2 \leqslant \sum_p \left(\frac{N}{p} + 1\right) = N^2 \sum \frac{1}{p^2} + 2N \sum \frac{1}{p} + r.$$

Как известно, сумма обратных квадратов к простым числам меньше 0,498, а сумма обратных к простым не больше $a \ln M < 0{,}001N^2$ для некоторой константы a и больших n. Значит, данная сумма не больше $N^2/2$. Поэтому при достаточно больших n хотя бы в половине клеток таблицы стоят простые числа, большие $0{,}001N^2$. По принцип Дирихле найдется такой ряд, в котором больше половины таких простых чисел. А раз так, то соответствующее число, стоящее напротив этого ряда ($a + i$ или $b + j$) не меньше $M^{N/2} > (0{,}001n^2)^{n/2} = (cn)^n$.

Осталось заметить, что, во-первых, аналогичное неравенство выполнено и для чисел a И b (для этого, возможно, потребуется уменьшить константу c), а во-вторых, оно выполнено не только для достаточно больших n, но и при всех натуральных (для этого потребуется, возможно, еще раз уменьшить константу c).