ПРОСТЫЕ ЧИСЛА, LTE-ЛЕММА, ПЕРВООБРАЗНЫЕ КОРНИ И КРУГОВЫЕ МНОГОЧЛЕНЫ

П. В. Бибиков[1]

Содержание

1. Введение

Данное пособие посвящено различным темам, связанным с рассмотрением простых чисел и остатков степеней натуральных чисел по различным модулям. Помимо классических малой теоремы Ферма и теоремы Эйлера, а также теоремы Евклида о бесконечности множества простых чисел, в олимпиадной литературе зачастую отсутствуют какие-либо иные способы работы с такими задачами. Между тем, в задачах высокого уровня этих фактов уже не хватает, и в результате школьники, не зная заранее нужных методов, вынуждены изобретать их на ходу, хотя было бы достаточно сослаться на готовое утверждение.

В этом пособии разобраны такие малоизвестные темы. С одной стороны, каждая из них выглядит достаточно сложной для освоения (например, в некоторых требуются бином Ньютона и комплексные числа, лемма Гаусса и алгоритм Евклида). Но с другой, потратив некоторое время и разобравшись в теоретических аспектах, можно превратить процесс решения даже очень сложных задач в жонглирование заготовленными фактами, которые позволяют решать задачи уровня Международной математической олимпиады, просто последовательно ссылаясь на 2-3 известных факта.

Среди наиболее важных методов и понятий, позволяющих работать со степенями натуральных чисел, мы выделяем прежде всего следующие:

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

- бесконечность множеств простых делителей чисел специального вида;
- порядок числа по модулю;
- LTE-лемма;
- первообразные корни;
- круговые многочлены;
- теорема Зигмонди.

Мы последовательно проработаем эти темы, дав необходимые для решения задач теоретические сведения, а также приведя в конце подробные решения всех задач. Кроме того, учитывая разнообразие конструкций, использующихся при работе с данными методами, их освоение полезно и для тренировки применения стандартных алгебраических фактов, методов и преобразований.

2. Простые делители

Мы начнем наш путь с такого, казалось бы, простого вопроса, как бесконечность множества простых делителей чисел определенного вида. Оказывается, что во многих задачах подобного типа есть некоторая общая идеология, проследив которую, можно научиться решать даже очень трудные на первый взгляд примеры.

1. (теорема Евклида) Простых чисел бесконечно много.

Несмотря на кажущуюся простоту доказательства этой теоремы, в ней есть несколько неочевидных соображений, которые полезно зафиксировать для дальнейших нужд.

- Простые числа являются более сложным объектом, нежели числа натуральные. В алгебраических (и не только) задачах полезно стартовать с самой сложной части условия: разобравшись с ней, скорее всего, удастся серьезно продвинуться и во всем решении. Поэтому в качестве стартового объекта полезно фиксировать *простые числа*, а не *натуральные*. Мы по *простому числу* строим *натуральное*, обладающее нужным нам свойством, а не ищем натуральное число, имеющее нужный нам простой делитель.
- Часто бесконечность какого-либо множества простых чисел полезно доказывать от противного, предполагая его конечность и строя новое простое число.
- Для построения нового простого числа полезно перемножать уже имеющиеся простые.

Держа в уме эти соображения, давайте попробуем справиться с остальными задачами.

2. Докажите, что существует бесконечно много простых чисел вида $4k-1$, где $k \in \mathbb{N}$.

3. Существует ли 2019 последовательных натуральных чисел, среди которых есть в точности 10 простых?

4. Пусть $f \in \mathbb{Z}[x]$ — целочисленный многочлен степени $\geqslant 1$, и P — множество простых делителей чисел вида $f(n)$, где $n \in \mathbb{N}$. Докажите, что множество P всегда бесконечно.

5. Пусть $f \in \mathbb{Z}[x]$ — целочисленный многочлен, такой, что $f(n) > 1$ для всех натуральных n, а $p(n)$ — наибольший простой делитель числа $f(n)$. Докажите, что существует бесконечно много

n, таких, что $p(n+1) > p(n)$.

6. Пусть $a > b \geqslant 1$ — натуральные числа и P — множество всех простых делителей чисел вида $a^n + b^n$. Докажите, что множество P бесконечно.

Замечание 1. На самом деле верно гораздо более сильное утверждение: взяв *любую* новую степень, можно получить *новый простой делитель* числа $a^n + b^n$ (за исключением нескольких случаев, которые конкретно описываются). Соответствующее утверждение называется *теоремой Зигмонди*, и для доказательства нам потребуется довольно мощная техника. Мы обсудим эту теорему позднее.

7. Пусть $G \neq \mathbb{Z}_n^*$ — подгруппа обратимых элементов по натуральному модулю n. Тогда множество простых чисел, остатки от деления которых на n не принадлежат группе G, бесконечно. В частности, простых чисел, не представимых в виде $nk+1$, бесконечно много (например, простых вида $4k-1$ или $6k-1$).

8. Пусть $2 \leqslant a, b \leqslant 100$ — два натуральных числа. Докажите, что существует такое натуральное n, что число $a^{2^n} + b^{2^n}$ составное.

9. Пусть $p(n)$ — наибольший простой делитель числа n^2+1. Докажите, что существует бесконечно много троек (a, b, c), таких, что $p(a) = p(b) = p(c)$.

10. Докажите, что существует бесконечно много натуральных n, таких, что наибольший простой делитель числа n^2+1 больше

а) $2n$

б) $2n + \sqrt{2n}$.

11. Пусть $p(n)$ — наибольший простой делитель числа n. Докажите, что существует бесконечно много натуральных n, таких, что $p(n) < p(n+1) < p(n+2)$.

12. Пусть $p(n)$ — наибольший простой делитель числа n (также положим $p(\pm 1) = 1$ и $p(0) = \infty$). Найти все целочисленные многочлены $f \in \mathbb{Z}[x]$, такие, что множество $\{p(f(n^2)) - 2n\}_{n \geqslant 0}$ ограничено сверху.

13. Пусть $f(x) = x^2 + x + a$, где $a \in \mathbb{N}$ — произвольное натуральное число. Докажите, что если числа $f(0)$, $f(1)$, …, $f([\sqrt{a/3}])$ простые, то все числа $f(0)$, $f(1)$, …, $f(a-2)$ простые.

3. Порядок числа по модулю

В этом разделе мы рассмотрим красивую конструкцию, которая по существу является альтернативной формой записи малой теоремы Ферма и теоремы Эйлера. Однако иногда бывают ситуации, когда требуется именно такая форма записи, поэтому нужно знать ее и уметь применять.

Напомним, что *порядком числа a по модулю m* называется такое *наименьшее* натуральное T, что $a^T \equiv 1 \pmod{m}$.

В чем заключается альтернативная форма записи малой теоремы Ферма и теоремы Эйлера? Напомним, что малая теорема Ферма звучит так: если p — простое число, a — целое, такое, что $p \nmid a$, то $a^{p-1} \equiv 1 \pmod{p}$. В случае, если вместо простого числа рассматривается произвольное натуральное m, получается теорема Эйлера: если $(a, m) = 1$, то $a^{\varphi(m)} \equiv 1 \pmod{m}$, где φ — *функция Эйлера*, ставящая в соответствие натуральному числу m количество чисел, меньших m и взаимно простых с ним (или, иначе говоря, количество обратимых элементов по модулю m: $\varphi(m) = |\mathbb{Z}_m^*|$). Для вычисления функции Эйлера нужно помнить, что она мультипликативна, т.е. если $(m, k) = 1$, то $\varphi(mk) = \varphi(m) \cdot \varphi(k)$, и что $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$.

Смысл применения порядка числа заключается в следующем наблюдении: $T \mid \varphi(m)$ (или $T \mid p-1$, если модуль прост). Таким образом, это понятие позволяет усилить малую теорему Ферма (или теорему Эйлера), извлекая из нее дополнительную информацию, которую затем удается применить. Поэтому решения многих задач полезно начинать со следующих ходов. Перепишем условие задачи в виде $a^k \equiv 1 \pmod p$ (здесь нужно правильно выбрать числа a, k и p) и рассмотрим порядок T числа a по модулю p. Тогда $T \mid k$ (т.к. T — наименьшая степень, дающая 1) и $T \mid p-1$ (по малой теореме Ферма). Дальше идут рассуждения, связанные именно с делимостями, как правило, без привлечения степеней.

14. Докажите, что если p — простое, то у числа 2^p-1 все простые делители больше p.

15. Докажите, что если p — простое, то любой простой делитель числа 2^p-1 имеет вид $2kp+1$ для некоторого натурального k.

16. а) Пусть p — нечетный простой делитель числа $a^{2^n}+1$. Докажите, что $2^{n+1} \mid p-1$.

б) Докажите, что все простые делители чисел Ферма $2^{2^n}+1$ имеют вид $2^{n+1} \cdot x + 1$.

17. Докажите, что для любого натурального n число 2^n-1 не делится на n.

18. Существует ли набор натуральных чисел $(n_1, \ldots, n_k)$, такой, что $n_i > 1$ и $n_i \mid 2^{n_{i+1}}-1$ для всех $i = 1, \ldots, k$ (мы считаем, что $n_{k+1} = n_1$)?

19. а) Известно, что $p \neq 2$, q, r — простые числа, такие, что $p \mid q^r+1$. Докажите, что либо $2r \mid p-1$, либо $p \mid q^2-1$.

б) Найдите все тройки простых чисел (p,q,r), такие, что $p \mid q^r+1$, $q \mid r^p+1$, $r \mid p^q+1$.

20. Найти все пары простых чисел $(p;q)$, таких, что $pq \mid (5^p-2^p)(5^q-2^q)$.

21. Найти все пары простых чисел p, q, таких, что $pq \mid 2^p+2^q$.

22. Найти все натуральные n, такие, что наборы простых делителей у чисел n и 2^n+1 совпадают.

4. LTE-лемма

При решении последнего номера из предыдущего раздела нам пришлось рассматривать максимальную степень вхождения числа 2 в разложения чисел $p-1$ и $q-1$ на простые сомножители. Оказывается, что идея рассмотрения степени вхождения данного простого числа p в ту или иную комбинацию степеней является одним из основных инструментов работы с ними. В этом разделе мы придадим четкий смысл этим словам и докажем важную теорему, позволяющую реализовывать эту идею на практике.

Для простого числа p и целого ненулевого числа x обозначим через $\|x\|_p$ наибольшую степень p, на которую делится x:

$$\|x\|_p = \alpha \quad \Leftrightarrow \quad p^\alpha | x, \quad p^{\alpha+1} \nmid x.$$

В этом случае также используется обозначение $p^\alpha \| x$. Напомним, что согласно формуле Лежандра

$$\|n!\|_p = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \ldots$$

23. Докажите, что

$$\|C_n^k\|_p > \|n\|_p - \frac{k}{p-1}.$$

24. Пусть n нечетно и $3^\alpha \| n$. Докажите, что $3^{\alpha+1} \| 2^n+1$.

Эта задача является частным случаем так называемой *леммы о лифтинге*, или *леммы об уточнении показателя* (в оригинале — **Lifting The Exponent Lemma**, сокращенно **LTE**), которая часто фигурирует в олимпиадных задачах по теории чисел.

Теорема 1 (LTE-лемма). *1. Пусть x и y — различные ненулевые целые числа, p — нечетное простое число, не являющееся делителем x и y и такое, что $p \mid x - y$. Тогда для любого натурального n выполнено равенство*

$$\|x^n - y^n\|_p = \|x - y\|_p + \|n\|_p.$$

2. Пусть x и y — различные целые числа, p — нечетное простое число, не являющееся делителем x и y и такое, что $p \mid x+y$. Тогда для любого нечетного натурального n выполнено

$$\|x^n + y^n\|_p = \|x + y\|_p + \|n\|_p.$$

3. Пусть x и y — различные нечетные целые числа и $4 \mid x - y$. Тогда для любого натурального n выполнено

$$\|x^n - y^n\|_2 = \|x - y\|_2 + \|n\|_2.$$

Следствие 1. 1. Пусть числа $a \geqslant 2$, α и n — натуральные, $\beta \geqslant 0$ — целое и $p \geqslant 3$ — простое. Если $p^\alpha \| a - 1$ и $p^\beta \| n$, то $p^{\alpha+\beta} \| a^n - 1$.

2. Пусть числа a, α, $\beta \geqslant 0$ — целые, $p \geqslant 3$ — простое. Если $p^\alpha \| a + 1$ и $p^\beta \| n$ для нечетного натурального n, то $p^{\alpha+\beta} \| a^n + 1$.

3. Если $2^\alpha \| a - 1$ при $\alpha \geqslant 0$ и $2^\beta \| n$, то $p^{\alpha+\beta} \| a^n - 1$.

Замечание 2. В таком виде эта теорема объясняет название «лифтинг»: полагая $n = p^\beta$, получаем, что $p^{\alpha+\beta} \| a^{p^\beta} - 1$, т.е. p^β поднимается наверх в степень.

25. Докажите LTE-лемму.

26. Пусть натуральные числа x, y, p, n, k таковы, что $x^n + y^n = p^k$. Докажите, что если число $n > 1$ — нечетное, а число p — простое нечетное, то n является степенью числа p с натуральным показателем.

27. Решить уравнение $3^x = 2^x \cdot y + 1$ в натуральных числах.

28. Найдите все такие натуральные n, что при некоторых взаимно простых x и y и натуральном $k > 1$ выполняется равенство $3^n = x^k + y^k$.

29. На сколько нулей заканчивается число $4^{5^6} + 6^{5^4}$?

30. Найти максимальную степень k числа 1991, для которой $1991^k \mid 1990^{1991^{1992}} + 1992^{1991^{1990}}$.

31. Докажите, что для любого натурального $a > 2$ найдется такое натуральное $n > 1$, что $a^n - 1$ делится на n^2. Верно ли это утверждение для $a = 2$?

5. Первообразные корни

Важным примером работы порядка числа по модулю является следующая ситуация. Как мы уже знаем из первого раздела, порядок любого числа по модулю m является делителем числа $\varphi(m)$ (в случае $m = p$ простого модуля порядок является делителем числа $p - 1$). Оказывается, иногда существует такое число g, чей порядок *равен* $\varphi(m)$. Иначе говоря, все числа 1, g, g^2, …, $g^{\varphi(m)-1}$ различны по модулю m. Такое число называется *первообразным корнем по модулю m*,

и его использование часто бывает необходимо в задачах, связанных с рассмотрением степеней натуральных чисел.

Прежде всего нам нужно узнать некоторые основные свойства первообразных корней, а также понять, для каких модулей m они в принципе существуют.

32. Докажите, что 2 — первообразный корень по модулю 3^n.

33. Пусть g — первообразный корень по модулю p. Докажите, что или g, или $g+p$ является первообразным корнем по модулю p^2.

34. Пусть g — нечетный первообразный корень по модулю простого числа p, причем $g^{p-1}-1$ не делится на p^2. Докажите, что g является первообразным корнем по модулям p^n и $2p^n$.

35. Пусть g — первообразный корень по модулю p. Докажите, что существует такое целое t, что число $g+tp$ является первообразным корнем по модулю p^n для любого n.

Теперь докажем следующее утверждение.

Теорема 2. *Первообразные корни существуют лишь по модулям* 2, 4, p^n *и* $2p^n$, *где* p — *нечетное простое число, а* n — *натуральное.*

36. Докажите, что для отличных от указанных в теореме модулей первообразных корней не существует.

37. Докажем, что первообразный корень существует для любого простого модуля p. Для этого последовательно докажем следующие утверждения.

а) Над $\mathbb{Z}_p$ (где p — простое) многочлен степени d имеет не более d корней.

б) Пусть ab — порядок числа x по модулю m. Тогда b — порядок числа x^a по модулю m.

в) Пусть $d_1, \ldots, d_k$ — всевозможные порядки всех вычетов по модулю p. Рассмотрим $h = [d_1, \ldots, d_k]$. Используя разложение числа h на простые сомножители, докажите существование первообразного корня по модулю p.

38. Докажите, что первообразных корней по модулю m ровно $\varphi(\varphi(m))$ штук (если они есть).

39. Пусть p — простое число. Для каких натуральных k имеет место сравнение

$$\sum_{i=1}^{p-1} i^k \equiv 0 \pmod{p}?$$

40. Пусть p — простое число. Докажите, что числа 1, 2, …, $p-1$ можно расставить по кругу так, чтобы для любых стоящих рядом чисел a, b, c число b^2-ac не делилось бы на p.

41. Докажите, что для любого натурального n найдется такое натуральное m, что $3^n \mid 2^m+2018$.

6. Круговые многочлены

При работе со степенями натуральных чисел невероятным образом оказываются полезны так называемые *круговые многочлены*, или *многочлены деления круга*. Вообще использование многочленов в теории чисел встречаются не так уж и редко, но зачастую эти многочлены определяются довольно просто. А вот многочлены деления круга определяются с помощью комплексных чисел…

Напомним, что *корнем* n*-й степени из единицы* называется такое комплексное число ξ, что $\xi^n = 1$. Корней n-й степени из 1 существует ровно n штук, и равны они

$$\xi_k := \cos\frac{2\pi k}{n} + i\sin\frac{2\pi k}{n} = e^{\frac{2\pi i k}{n}}, \quad \text{где } k = 0, 1, \ldots, n-1.$$

Круговым многочленом порядка n называется многочлен

$$\Phi_n(x) = \prod_{(k,n)=1} (x - \xi_k),$$

где ξ_k — корни n-й степени из 1. Именно эти, на первый взгляд, странные многочлены оказываются очень полезны при решении различных задач по теории чисел.

Начнем с того, что докажем основные свойства круговых многочленов.

42. Докажите, что если p — простое, то $\Phi_p(x) = 1 + x + x^2 + \ldots + x^{p-1}$.

43. Докажите, что $\prod\limits_{d|n} \Phi_d(x) = x^n - 1$. В частности, $\Phi_n(x) \mid x^n - 1$ и $\sum\limits_{d|n} \varphi(d) = n$.

44. Докажите, что $\Phi_n(x) \in \mathbb{Z}[x]$.

45. а) Пусть p — произвольное простое число. Докажите, что

$$\Phi_{pn}(x) = \begin{cases} \Phi_n(x^p), & \text{если } p \mid n, \\ \frac{\Phi_n(x^p)}{\Phi_n(x)}, & \text{если } p \nmid n \end{cases} \qquad \text{и} \quad \Phi_{p^k n}(x) = \begin{cases} \Phi_n(x^{p^k}), & \text{если } p \mid n, \\ \frac{\Phi_n(x^{p^k})}{\Phi_n(x^{p^{k-1}})}, & \text{если } p \nmid n. \end{cases}$$

б) Докажите, что при $(n, k) = 1$ имеет место равенство

$$\Phi_n(x^k) = \prod_{d|k} \Phi_{nd}(x).$$

46. Докажите, что $\Phi_n(x) \;\Big|\; \dfrac{x^n - 1}{x^k - 1}$ при $k \mid n$ и $k \neq n$.

47. Пусть p — простой делитель числа $\Phi_n(a)$. Тогда $n = p^\alpha q$, где $\alpha \geqslant 0$ и q — показатель числа a по модулю p.

48. Докажите, что если числа $\Phi_n(a)$ и $\Phi_m(a)$ не взаимно просты, то $\frac{m}{n}$ является степенью некоторого простого числа (возможно отрицательной).

49. Пусть a и n — целые числа и p — простой делитель $\Phi_n(a)$. Докажите, что либо $p \mid n$, либо $n \mid p - 1$.

Теперь посмотрим, как круговые многочлены помогают решать различные задачи. Ключевым обычно является следующее соображение. Если в условии присутствует выражение вида $m^n - 1$, то нужно рассмотреть число $\Phi_n(m)$, являющееся его делителем, и простые числа, делящие $\Phi_n(m)$. Об этих простых числах у нас есть существенная информация, которую можно использовать. При этом часто бывает полезно воспользоваться алгоритмом Евклида для степеней: $(a^n - 1, a^m - 1) = a^{(n,m)} - 1$.

50. Докажите, что для любого натурального n существует) бесконечно много простых чисел p, таких, что $n \mid p - 1$.

51. Пусть p — простое число. Докажите, что существует такое простое число q, что для любого натурального n число $n^p - p$ не делится на q.

52. Пусть $p_1, \ldots, p_k$ — различные простые числа, большие 3, и $N = 2^{p_1 \cdots p_k} + 1$. Докажите, что у числа N есть хотя бы 2^{2^k} делителей.

53. Решить уравнение $\dfrac{x^7 - 1}{x - 1} = y^5 - 1$ в целых числах.

54. Докажите, что мультипликативная группа $\mathbb{K}^\times$ любого конечного поля $\mathbb{K}$ является цикли-

ческой.

55. Для каждого натурального k рассмотрим операцию f_k, определенную следующим образом:

$$f_k(n) = \left[\sqrt[k]{\text{наибольший простой делитель числа } (n^{2018k}+1)}\right].$$

Докажите, что с помощью нескольких таких операций каждое натуральное число можно привести к 1 (в качестве k можно взять любое натуральное число и менять его при необходимости).

7. Неприводимость круговых многочленов

Основная роль круговых многочленов — разложение на множители выражения $x^n - 1$ и извлечение информации о простых делителях этого выражения. В следующем разделе мы докажем одну из самых мощных теорем в этой области, применение которой делает многие задачи, содержащие выражения вида $a^n - 1$, практически очевидными. Сейчас же мы ответим на другой вопрос, также представляющий интерес: является ли разложение

$$x^n - 1 = \prod_{d|n} \Phi_d(x)$$

многочлена $x^n - 1$ разложением на *неприводимые* множители? Иначе говоря, верно ли, что многочлены Φ_n неприводимы над $\mathbb{Q}$? Это действительно верно, однако доказательство весьма непросто.

Теорема 3. *Круговые многочлены Φ_n неприводимы над $\mathbb{Q}$ для любого n.*

Доказательство мы проедем в несколько этапов.

56. (критерий Эйзенштейна) Пусть $P(x)$ — приведенный многочлен с целыми коэффициентами, причем все его коэффициенты, кроме старшего, делятся на некоторое простое p, а свободный член не делится на p^2. Докажите, что многочлен $P(x)$ неприводим над $\mathbb{Q}$.

57. Докажите, что для простого p многочлен $\Phi_p(x)$ неприводим над $\mathbb{Q}$.

58. Предположим, что $\Phi_n(x) = \prod\limits_{i=1}^{s} Q_i(x)$, где $Q_i \in \mathbb{Q}[x]$ неприводимы и $s > 1$. Пусть также $m = \deg Q_1 \leqslant \deg Q_i$ для всех i.

а) Обозначим через $x_1, \ldots, x_m$ (комплексные) корни многочлена Q_1. Докажите, что для любого k многочлен $\widetilde{Q}_k(x) = \prod\limits_{i=1}^{m}(x - x_i^k)$ имеет целые коэффициенты.

б) Докажите, что $\Phi_n = \prod\limits_{k:(k,n)=1} \widetilde{Q}_k$.

в) Докажите, что существует такое k, что $\widetilde{Q}_k \neq Q_1$ и при этом сравнение $p \equiv k \pmod{n}$ имеет бесконечно много решений в простых числах.

г) Завершите доказательство теоремы о неприводимости круговых многочленов.

8. Теорема Зигмонди

Теорема, которую мы сейчас докажем, является, возможно, самой мощной теоремой в олимпиадной теории чисел, связанной со степенями натуральных. Эта теорема позволяет решать задачи, казалось бы, невероятной сложности, практически сразу. Разумеется, за такую легкость

придется заплатить. В данном случае платой будет чрезвычайная сложность доказательства, а также понимание того, что составители олимпиад знают об этой теореме, а потому стараются предлагать задачи, в которых эта теорема неприменима. Тем не менее, знать ее необходимо.

Теорема 4 (Зигмонди). *1. Пусть $a > b$ — натуральные числа. Тогда для любого натурального $n \geqslant 2$ число $a^n - b^n$ содержит в своем разложении на простые сомножители такое простое, которого нет в разложении чисел $a^k - b^k$ для всех $k < n$. Исключения составляют следующие два случая:*

- $n = 2$, $a + b = 2^m$;
- $n = 6$, $a = 2$, $b = 1$.

2. Пусть $a > b$ — натуральные числа. Тогда для любого натурального $n \geqslant 2$ число $a^n + b^n$ содержит в своем разложении на простые сомножители такое простое, которого нет в разложении чисел $a^k + b^k$ для всех $k < n$. Исключения составляет следующий случай:

- $n = 3$, $a = 2$, $b = 1$.

Мы разобьем доказательство этой теоремы на несколько шагов. Прежде всего докажем теорему Зигмонди для случая $b = 1$. Назовем простое число p, делящее $a^n - 1$ и не делящее $a^k - 1$ при всех $k < n$, *примитивным*. Мы хотим доказать, что при всех a и n, за исключением случаев, указанных в теореме, у числа $\Phi_n(a)$ есть примитивный простой делитель (т.к. $\Phi_n(a) \mid a^n - 1$, этот же простой делитель будет и у числа $a^n - 1$). Основной идеей доказательства является оценка числа $\Phi_n(a)$ снизу через его простой делитель, не являющийся примитивным: мы докажем, что $\Phi_n(a) > p$ и $\|\Phi_n(a)\|_p = 1$, за исключением двух случаев, указанных в теореме.

Итак, предположим, что у числа $\Phi_n(a)$ нет примитивных простых делителей. Пусть $p \mid \Phi_n(a)$ — некоторый простой делитель. Тогда существует число $k \mid n$, такое, что $p \mid a^k - 1$.

59. Пусть $n = p^\alpha q$, где $p \nmid q$. Докажите, что $\alpha > 0$. Отсюда следует, что p — *наибольший простой делитель* числа n.

60. Докажите, что если $p = 2$, то $n = 2$ и $a + b$ — степень двойки.

61. Докажите, что если $p > 2$, то $\|\Phi_n(a)\|_p = 1$.

Из последней задачи следует, что для доказательства теоремы Зигмонди достаточно доказать, что $\Phi_n(a) > p$. В самом деле, $\Phi_n(a)$ не может быть кратно p^2, т.к. $\|\Phi_n(a, b)\|_p = 1$, поэтому у числа $\Phi_n(a)$ должен найтись еще один простой делитель. Он также обязан быть непримитивным, а значит, по задаче **59** он должен быть наибольшим простым делителем n, что невозможно.

62. Пусть $n = p^\alpha q$, где $p \nmid q$.
а) Докажите, что $\Phi_n(a) > p$ при $\alpha > 1$.
б) Докажите, что $\Phi_n(a) > p$ при $\alpha = 1$ и $a > 2$.
в) Докажите, что $\Phi_n(a) > p$ при $\alpha = 1$ и $a = 2$, за исключением случая $n = 6$.

63. Докажите п.1 теоремы Зигмонди для произвольных a и b.

64. Докажите п.2 теоремы Зигмонди.

Теперь посмотрим, как теорема Зигмонди позволяет решать, казалось бы, очень трудные и громоздкие задачи.

65. Найти все решения уравнения

$$a^n - 1 = (a^p - 1)(a^q - 1)(a^r - 1)$$

в натуральных числах.

66. Найти все натуральных числа a, m, n, такие, что $a^m + 1 \mid (a+1)^n$.

67. Найти все такие натуральны числа x, p, n, r, такие, что p простое, n, $r > 1$ и $x^r - 1 = p^n$.

68. Найти все натуральные решения уравнения $p^x - y^p = 1$, где p — простое.

69. Решить уравнение $5^x - 3^y = z^2$ в натуральных числах.

70. Найти все натуральные решения уравнения $p^a - 1 = 2^n(p-1)$, где p — простое.

71. Решить уравнение

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

в натуральных числах.

9. Разные задачи

72. Докажите, что существует такое натуральное n, что $8^n + 2018$ делится на 5^{2018}.

73. Существует ли такое натуральное N, что у числа N в точности 2019 простых делителей и $N \mid 2^N + 1$?

74. Пусть N — натуральное число, заканчивающееся на 25, а m — произвольное натуральное число. Докажите, что существует такое натуральное n, что у m последних цифр в записи чисел N и 5^n совпадают четности, а у $(m+1)$-ых цифр четности различны.

75. Пусть p — простое число и a, n — натуральные числа. Докажите, что если $2^p + 3^p = a^n$, то $n = 1$.

76. Докажите, что разность $3^n - 2^n$ не делится на n ни для какого натурального n.

77. Докажите, что если $3^n - 2^n = p^a$ для некоторых натуральных n, a и простого p, то тогда n — простое.

78. Докажите, что существует бесконечно много составных чисел n, таких, что выполнено следующее свойство: если $n \mid a^n - 1$, то $n^2 \mid a^n - 1$ для любого натурального a.

79. Найдите все натуральные $n > 1$, такие, что число $\dfrac{2^n+1}{n^2}$ является целым.

80. Пусть b, m, n — натуральные числа, такие, что $b > 1$ и $m \neq n$. Докажите, что если $b^m - 1$ и $b^n - 1$ имеют одинаковый набор простых делителей, то $b+1$ является степенью двойки.

81. Докажите, что все числа

$$10001, \quad 100010001, \quad 1000100010001, \quad \ldots$$

являются составными.

82. Найти все тройки (p, x, y), состоящие из простого числа p и двух натуральных чисел x и y, таких, что $x^{p-1} + y$ и $x + y^{p-1}$ являются степенями числа p.

83. Пусть m — нечетное натуральное число, $m > 3$. Найти наименьшее натуральное n, такое, что $2^{2019} \mid m^n - 1$.

84. Докажите, что существует бесконечно много натуральных n, таких, что все простые дели-

тели числа n^2+1 меньше $\sqrt{n}$.

85. Найти все натуральные числа n и p, такие, что p — простое, $n \leqslant 2p$ и $n^{p-1} \mid (p-1)^n + 1$.

86. Для каждого натурального k обозначим через $C(k)$ сумму всех простых различных делителей числа k. Например $C(1) = 0$, $C(2) = 2$, $C(45) = 8$. Найдите все натуральные n для которых $C(2^n + 1) = C(n)$.

87. Пусть n — произвольное натуральное число. Докажите, что у числа $2^{2^n} + 2^{2^{n-1}} + 1$ есть не менее 2^n натуральных делителей.

88. Найдите все натуральные k такие, что произведение первых k простых чисел, уменьшенное на 1, является точной степенью натурального числа (большей, чем первая).

89. Дано натуральное $k > 1$. Докажите, что существует бесконечно много натуральных n таких, что $n \mid 1^n + 2^n + 3^n + \ldots + k^n$.

90. Докажите, что последовательность $a_n = 3^n - 2^n$ не содержит трех последовательных членов геометрической прогрессии.

91. Докажите, что уравнение $x^n + y^n = p^n$ не имеет натуральных решений при $n \geqslant 3$ и простом p.

92. Докажите, что для любого простого p многочлен $x^4 + 1$ приводим над полем $\mathbb{Z}_p$.

93. Пусть $\{a_n\}$ — монотонно возрастающая последовательность натуральных чисел. Докажите, что множество простых делителей чисел вида $a_i + a_j$ (где $i \neq j$) бесконечно.

10. Решения задач

10.1. Простые делители

1. (теорема Евклида) Простых чисел бесконечно много.

Решение. Предположим противное: пусть простых чисел конечное число. Обозначим их через $p_1, \ldots, p_n$. Рассмотрим число $P = p_1 \ldots p_n + 1$. Это число не делится ни на одно из p_i. Рассмотрим наименьший натуральный делитель P, отличный от 1. Ясно, что тогда этот делитель является простым числом, отличным от уже имеющихся — противоречие.

2. Докажите, что существует бесконечно много простых чисел виде $4k - 1$, где $k \in \mathbb{N}$.

Решение. Будем рассуждать по аналогии с доказательством теоремы Евклида. Предположим, что простых чисел вида $4k - 1$ конечное число. Обозначим их через $p_1, \ldots, p_n$. Рассмотрим число $P = 4p_1 \ldots p_n - 1$. Заметим, что оно не делится ни на одно из чисел $p_1, \ldots, p_n$. С другой стороны, все простые делители не могут иметь вид $4k + 1$, потому что тогда их произведение также имеет вид $3k + 1$, что невозможно. Значит, у числа P существует простой делитель вида $4k - 1$, отличный от $p_1, \ldots, p_n$, что и дает нам противоречие.

3. Существует ли 2019 последовательных натуральных чисел, среди которых есть в точности 10 простых?

Решение. Заметим, что среди первых 2019 натуральных чисел есть 111 простых чисел: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31. С другой стороны, среди 2019 чисел $2020! + 2$, $2020! + 3$, $\ldots$, $2020! + 2020$ нет ни одного простого числа. Сдвигаясь на один шаг вправо по натуральном ряду от первого набора ко второму, мы изменяем количество простых чисел в наборе не более чем

на 1. Значит, найдется момент, когда мы получим набор, содержащий в точности 10 простых чисел, что и требовало доказать.

4. Пусть $f \in \mathbb{Z}[x]$ — целочисленный многочлен степени $\geqslant 1$, и P — множество простых делителей чисел вида $f(n)$, где $n \in \mathbb{N}$. Докажите, что множество P всегда бесконечно.

Решение. Пусть a_0 — свободный коэффициент многочлена f. Предположим, что существует лишь конечное число простых делителей значений многочлена f в целых точках. Обозначим эти делители через $p_1, \ldots, p_k$. Рассмотрим число $f\big(|a_0|(p_1 \ldots p_k)^m\big)$, где m выбрано настолько большим, что это число больше $|a_0|$ по модулю. Заметим, что это число равно

$$a_0\big(p_1 \ldots p_n(\ldots) \pm 1\big).$$

Ясно, что число в скобке больше 1 по модулю и не делится ни на одно из простых чисел $p_1, \ldots, p_k$. Значит, у него есть простой делитель, отличный от $p_1, \ldots, p_k$ — противоречие.

5. Пусть $f \in \mathbb{Z}[x]$ — целочисленный многочлен, такой, что $f(n) > 1$ для всех натуральных n, а $p(n)$ — наибольший простой делитель числа $f(n)$. Докажите, что существует бесконечно много n, таких, что $p(n+1) > p(n)$.

Решение. Предположим противное: пусть таких n лишь конечное число, и N — наибольшее из них. Тогда $p(N) \geqslant p(N+1) \geqslant p(N+2) \geqslant \ldots$. Но тогда у значений многочлена f лишь конечное число простых делителей: те простые, которые делят $f(1), \ldots, f(N)$, и некоторые из простых, меньших $p(N)$ — противоречие с задачей 4.

6. Пусть $a > b \geqslant 1$ — натуральные числа и P — множество всех простых делителей чисел вида $a^n + b^n$. Докажите, что множество P бесконечно.

Решение. Способ 1. Без ограничения общности можно считать, что $(a, b) = 1$. Предположим противное: пусть простых делителей чисел вида $a^n + b^n$ лишь конечное число. Обозначим их через $p_1, \ldots, p_k$. Рассмотрим тогда число $N = (p_1 - 1) \ldots (p_k - 1)$. По малой теореме Ферма $a^N + b^N \equiv 2$ или $1 \pmod{p_i}$ для всех $i = 1, \ldots, k$. Второй случай сразу приводит к противоречию. В первом случае получается, что $i = 1$, $p_1 = 2$ и $a^N + b^N = 2^s$. Проводя аналогичные рассуждения для $2N$, заключаем, что $a^{2N} + b^{2N} = 2^r$. Значит, $2^r + 2(ab)^N = 2^{2s}$ и $2^{r-1} + (ab)^N = 2^{2s-1}$. Но числа a и b взаимно просты, а значит, оба нечетны, поэтому последнее равенство невозможно. Мы пришли к противоречию.

Способ 2. Будем искать простые делители у чисел вида $a^{2^m} + b^{2^m}$. Опять будем считать числа a и b взаимно простыми. Предположим, что у чисел такого вида конечное число простых делителей. Обозначим их через $p_1, \ldots, p_k$. Тогда, начиная с некоторого M, все числа вида $a^{2^m} + b^{2^m}$ имеют простые делители среди $p_1, \ldots, p_k$ для $m \geqslant M$. Заметим, что

$$a^{2^{M+1}} + b^{2^{M+1}} = (a-b)(a+b)\ldots\big(a^{2^M} + b^{2^M}\big) + 2b^{2^{M+1}}.$$

Значит, если $p \mid a^{2^{M+1}} + b^{2^{M+1}}$, то $p \mid 2b^{2^{M+1}}$ и $p = 2$. Значит, $a^{2^m} + b^{2^m}$ — степень двойки для всех $m > M$. Дальнейшая часть доказательства дословно повторяет рассуждения из предыдущего способа.

7. Пусть $G \neq \mathbb{Z}_n^*$ — подгруппа обратимых элементов по натуральному модулю n. Тогда множество простых чисел, остатки от деления которых на n не принадлежат группе G, бесконечно. В частности, простых чисел, не представимых в виде $nk+1$, бесконечно много (например, простых вида $4k - 1$ или $6k - 1$).

Решение. Предположим противное: пусть существует лишь конечное множество простых чисел указанного вида. Обозначим их через $p_1, \ldots, p_k$. Рассмотрим произвольное число $x \in \mathbb{Z}_n^* \setminus G$. По китайской теореме об остатках можно найти такое число y, что $y \equiv x \pmod{n}$ и $y \equiv 1 \pmod{}$

p_i) для всех i. Возьмем число $P = np_1 \dots p_n + y$. Ясно, что это число содержит простой делитель, не сравнимый с элементами G по модулю n и не совпадающий с $p_1, \dots, p_k$ — противоречие.

8. Пусть $2 \leqslant a, b \leqslant 100$ — два натуральных числа. Докажите, что существует такое натуральное n, что число $a^{2^n} + b^{2^n}$ составное.

Решение. Если $a = b$, то подходит $n = 1$, ибо $a^2 + b^2$ — четное число, большее 2. Далее мы предполагаем, что $a \neq b$. В этом случае мы установим, что при некотором n число $a^{2^n} + b^{2^n}$ делится на 257 и не равно 257.

Предположим, что если $a^{2^n} + b^{2^n} = 257$, то или a, или $b = 1$ (т.к. $16^2 + 1^2 = 257$ — единственное представление простого числа 257 в виде суммы двух квадратов). Но это невозможно, т.к. a и $b > 1$.

Ясно, что a и b не делятся на 257. Полагая $q \equiv \frac{a}{b} \pmod{257}$, докажем, что $q^{2^n} + 1$ делится на 257 для некоторого $n \leqslant 7$. Для этого заметим, что по малой теореме Ферма

$$q^{2^8} - 1 = (q-1)(q+1)(q^2+1)\dots\left(q^{2^7+1}\right) - 1 \equiv 0 \pmod{257}.$$

Т.к. $q \not\equiv 0, \pm 1 \pmod{257}$, получаем, что какая-то из скобок $q^{2^n} + 1$ кратна 257. Но тогда $a^{2^n} + b^{2^n} \equiv b^{2^n}(q^{2^n} + 1) \equiv 0 \pmod{257}$, что и требовалось доказать.

9. Пусть $p(n)$ — наибольший простой делитель числа $n^2 + 1$. Докажите, что существует бесконечно много троек (a, b, c), таких, что $p(a) = p(b) = p(c)$.

Решение. Способ 1. Достаточно доказать, что найдется бесконечно много простых чисел q, таких, что $q = p(n)$ и $q < n$. В самом деле, тогда положим $a = n$, b равным остатку a по модулю q и $c = q - b$. Чтобы найти такие q и n, рассмотрим решения уравнения Пелля $n^2 + 1 = 5m^2$, большие 5. Тогда $m < n$ и $p(n)$ равен или 5, или максимальном простому делителю числа m. И в том, и в другом случае $p(n) < n$. Значит, выбирая $a = n$, $q = p(n)$, b равным остатку a по модулю q и $c = q - b$, получаем искомую бесконечную серию примеров.

Способ 2. Пусть q — нечетное простое число, а $a < q$ — такое натуральное число, что $q \mid a^2 + 1$ (согласно задаче 4 таких пар чисел бесконечно много). Тогда числа a и $q - a$ различны и $p(a) = p(q - a)$. Действительно, числа $a^2 + 1$ и $(q-a)^2 + 1 = (a^2 + 1) + q(q - 2a)$ делятся на q и меньше q^2; значит, они не могут делиться на простые числа, большие q.

Предположим, что существует лишь конечное число простых чисел q, для которых уравнение $p(n) = q$ имеет хотя бы три натуральных решения. Обозначим через s максимальное такое простое число (если таких простых не существует, положим $s = 2$), а через S — произведение всех простых чисел, не превосходящих s.

Пусть $r = p(S)$; тогда r взаимно просто с S и потому $r > s$. Пусть a — остаток от деления S на r; тогда $r \mid a^2 + 1$ и $p(a) = p(r - a) = r$. Одно из чисел a и $r - a$ четно; обозначим его через b.

Число $(b + r)^2 + 1$ делится на $2r$, поэтому $q = p(b + r) \geqslant r$.

Если $q = r$, то уравнение $p(x) = r$ имеет три решения — b, rb, $r + b$, а это невозможно по предположению.

Если $q > r$, число $(b + r)^2 + 1$ делится на $2qr$. Это означает, что $q < b + r$ (в противном случае $(b + r)^2 + 1 \leqslant (2r - 1)q + 1 < 2qr$). Обозначая через c остаток от деления числа $b + r$ на q, получаем $p(c) = p(q - c) = p(b + r) = q > p > s$, что противоречит выбору s.

Способ 3. Положим $n = 2m^2$. Тогда

$$n^2 + 1 = 4m^4 + 1 = (2m^2 + 2m + 1)(2m^2 - 2m + 1).$$

Нам достаточно доказать, что каждая из скобок раскладывается в произведение натуральных чисел, меньших $2m^2$, поскольку тогда у числа $n^2 + 1$ максимальный простой делитель будет меньше n, и можно будет взять $a = n$, b равным остатку n по модулю p и $c = p - b$.

Ясно, что $2m^2-2m+1 < 2m^2$. Кроме того, при $m = 3$, число $2m^2+2m+1$ равно 25 и делится на 5. Тогда можно взять $m = 3 + 5k$, где $k = 0, 1, 2, \ldots$, и при таких m получаем разложение

$$2m^2 + 2m + 1 = 5 \cdot \frac{2m^2 + 2m + 1}{5}$$

числа $2m^2+2m+1$ на натуральные множители, каждый из которых меньше $2m^2$. Значит, числа $n = 2(3 + 5k)^2$ подходят.

10. Докажите, что существует бесконечно много натуральных n, таких, что наибольший простой делитель числа $n^2 + 1$ больше

а) $2n$

б) $2n + \sqrt{2n}$.

Решение. а) Ключевая идея здесь состоит в следующем. Мы опять попробуем зацепиться за самую сложную часть условия. В данном случае это максимальный простой делитель p. Понятно, что, фиксируя число n, найти максимальный простой делитель числа $n^2 + 1$ невозможно. Поэтому поступим по-другому: зафиксируем само простое число p и будем искать такие n, для которых p будет простым делителем.

Прежде всего заметим, что сравнение $n^2 + 1 \equiv 0 \pmod p$ разрешимо для бесконечно многих простых p (а именно, для всех $p \equiv 1 \pmod 4$). Возьмем теперь решение $n < p/2$. Тогда $p > 2n$, что и требовалось.

б) Этот пункт теперь почти мгновенно следует из п. а). Для этого положим $d = p - 2n$. Тогда $p \mid n^2 + 1 = (p - d)^2/4 + 1$, откуда $p \mid d^2 + 4$. Значит, $d^2 \geqslant p - 4 = 2n + (d - 4) \geqslant 2n$ при $d \geqslant 4$ и $p \geqslant 4^2 + 4 = 20$. Значит, для каждого $p \geqslant 20$, такого, что $p \equiv 1 \pmod 4$, найдется такое n, что $p \mid n^2 + 1$ и $p > 2n + \sqrt{2n}$, что и требовалось доказать.

11. Пусть $p(n)$ — наибольший простой делитель числа n. Докажите, что существует бесконечно много натуральных n, таких, что $p(n) < p(n + 1) < p(n + 2)$.

Решение. Для удобства положим $m = n + 1$ и будем искать такие m, что $p(m - 1) < p(m) < p(m+1)$. Идея заключается в том, чтобы искать $m = q^{2^k}$, где q — произвольное нечетное простое. Ясно, что при $k = 1$ $p(q^2 - 1) < q = p(q^2)$. Докажем, что существует такое ℓ, что $p(q^{2^\ell} - 1) > q$. Тогда выбирая наименьшее такое ℓ и полагая $k = \ell - 1$, мы получаем требуемое, т.к.

$$p(q^{2^{\ell-1}} - 1) < q = p(q^{2^{\ell-1}}) < p(q^{2^\ell} - 1) = p(q^{\ell-1} + 1).$$

Для этого достаточно показать, что множество простых делителей чисел вида $q^{2^k} - 1$ бесконечно. Это сразу следует из задачи **6**, ведь $q^{2^{n+1}} - 1 = \big(q^{2^n} - 1\big)\big(q^{2^n} + 1\big)$, а множество простых делителей чисел из второй скобки бесконечно. Таким образом, наше утверждение полностью доказано.

12. Пусть $p(n)$ — наибольший простой делитель числа n (также положим $p(\pm 1) = 1$ и $p(0) = \infty$). Найти все целочисленные многочлены $f \in \mathbb{Z}[x]$, такие, что множество $\{p(f(n^2)) - 2n\}_{n\geqslant 0}$ ограничено сверху.

Решение. Зафиксируем наименьшее натуральное число c, такое, что $p(f(n^2)) - 2n \leqslant 2c + 1$. Согласно задаче **4**, у чисел вида $f(n^2)$ существует бесконечно много простых делителей. Выберем простой делитель $q > c$, тогда $q-2n \leqslant 2c+1$ и $n \geqslant \frac{q-1}{2} - c$. Заменяя при необходимости число n на число $q - n$, можно считать, что $n \leqslant \frac{q-1}{2}$. Значит, найдется такое число k на отрезке $[0; c]$, что

$$0 \equiv f\Big(\big(\frac{q-1}{2} - k\big)^2\Big) \equiv f\Big(\big(k + \frac{1}{2}\big)^2\Big) \pmod q.$$

Значит, q является делителем числителя числа

$$\prod_{k=0}^{c} f\Big(\big(k+\frac{1}{2}\big)^2\Big).$$

Но если это число не равен 0, то таких q конечное число. Поэтому найдется такое число k_0 на отрезке $[0;c]$, что $f\Big(\big(k+\frac{1}{2}\big)^2\Big)=0$, т.е. $f(x)=(4x-(2k_0+1)^2)\cdot f_1(x)$. Применяя аналогичные рассуждения к многочлену f_1, получаем окончательный ответ: $f(x)=A\prod\limits_{2\nmid a}(4x-a^2)$.

Ответ: $f(x)=A\prod\limits_{2\nmid a}(4x-a^2)$.

13. Пусть $f(x)=x^2+x+a$, где $a\in\mathbb{N}$ — произвольное натуральное число. Докажите, что если числа $f(0)$, $f(1)$, …, $f([\sqrt{a/3}])$ простые, то все числа $f(0)$, $f(1)$, …, $f(a-2)$ простые.

Решение. Предположим противное и рассмотрим наименьшее натуральное число $k\leqslant a-2$, при котором число $f(k)$ составное. Пусть $q\mid f(k)$ — его наименьший простой делитель. Ясно, что $k>q$, т.к. в противном случае можно взять остаток r числа k по модулю q, и тогда $f(k)\equiv f(r)\equiv 0\pmod q$, причем $f(r)\geqslant a>k\geqslant q$, т.е. $f(r)$ также составное, причем $r<k$, что невозможно. Тогда $q>2k$, поскольку в противном случае $k>q-1-k\geqslant 0$ и

$$f(q-1-k)\equiv f(-k-1)=f(k)\equiv 0\pmod q,$$

причем

$$f(q-1-k)=(q-1-k)^2+(q-1-k)+a>q+a-k-1\geqslant q,$$

т.е. число $f(q-1-k)$ также составное.

Значит, $k\geqslant 2q+1$, откуда получаем неравенство

$$f(k)=k^2+k+a\geqslant q^2\geqslant(2k+1)^2.$$

Таким образом, $3k^2<3k^2+3k+1\leqslant a$ и $k\leqslant[\sqrt{a/3}]$ — противоречие.

10.2. Порядок числа по модулю

14. Докажите, что если p — простое, то у числа 2^p-1 все простые делители больше p.

Решение. Предположим противное: пусть $2^p\equiv 1\pmod q$ и $q\leqslant p$ — некоторый простой делитель числа 2^p-1. Пусть также T — порядок числа 2 по модулю q. Тогда $2^T\equiv 1\pmod q$ и $T\mid p$, откуда либо $T=1$, либо $T=p$. В первом случае получаем, что $2\equiv 1\pmod p$, что невозможно, а во втором случае получаем, что $T=p\mid q-1$ по малой теореме Ферма, откуда $p\leqslant q-1$ — противоречие.

15. Докажите, что если p — простое, то любой простой делитель числа 2^p-1 имеет вид $2kp+1$ для некоторого натурального k.

Решение. Пусть q — простой делитель числа 2^p-1. Если T — порядок числа 2 по модулю q, то $T\mid p$, откуда $T=1$ или $T=2$. В первом случае получаем, что $2\equiv 1\pmod q$, что невозможно, а во втором — что $p\mid q-1$ по малой теореме Ферма. Значит, $q-1=np$. Ясно, что q нечетно, поэтому $n=2k$ четно и $q=2kp+1$.

16. а) Пусть p — нечетный простой делитель числа $a^{2^n}+1$. Докажите, что $2^{n+1}|p-1$.

б) докажите, что все простые делители чисел Ферма $2^{2^n}+1$ имеют вид $2^{n+1}\cdot x+1$.

Решение. а) Пусть $a^{2^n} \equiv -1 \pmod p$. Тогда $a^{2^{n+1}} \equiv 1 \pmod p$. Пусть T — порядок числа a по модулю p. Получаем, что $T \mid 2^{n+1}$, т.е. $T = 2^k$ при некотором $k \in \mathbb{N}$. Если $k \leqslant n$, то $1 \equiv (a^{2^k})^{2^{n-k}} = a^{2^n} \equiv -1 \pmod p$ и $p = 2$, что невозможно. Значит, $T = 2^{n+1}$ и по малой теореме Ферма $2^{n+1} = T \mid p - 1$, что и требовалось доказать.

б) Этот пункт незамедлительно получается из п. а) подстановкой $a = 2$. Интересен он тем, что именно благодаря этому факту Л. Эйлер сумел доказать, что число $2^{2^5} + 1$ не является составным: у него существует простой делитель $641 = 2^6 \cdot 10 + 1$.

17. Докажите, что для любого натурального n число $2^n - 1$ не делится на n.

Решение. Предположим, что для некоторого натурального n число $2^n - 1$ делится на n. Рассмотрим наименьший простой делитель p числа n и порядок T числа 2 по модулю p. Тогда $2^n \equiv 1 \pmod p$, откуда $T \mid n$ и $T \mid p - 1$. Но тогда $T < p$ — делитель n, меньший p. Значит, $T = 1$ и $2 \equiv 1 \pmod p$ — противоречие.

18. Существует ли набор натуральных чисел $(n_1, \ldots, n_k)$, такой, что $n_i > 1$ и $n_i \mid 2^{n_{i+1}} - 1$ для всех $i = 1, \ldots, k$ (мы считаем, что $n_{k+1} = n_1$)?

Решение. Пусть p — наименьший простой делитель среди всех делителей чисел $n_1, \ldots, n_k$. Тогда $p \mid n_i \mid 2^{n_{i+1}} - 1$. Значит, $2^{n_{i+1}} \equiv 1 \pmod p$. Пусть T — порядок числа 2 по модулю p. Тогда $T < p$ и $T \mid n_{i+1}$. Если $T > 1$, то у числа n_{i+1} существует простой делитель (входящий в разложение T), меньший p, что невозможно. Значит, $T = 1$ и $2 \equiv 1 \pmod p$, что невозможно. Значит, искомых наборов не существует.

Ответ: не существует.

19. а) Известно, что $p \neq 2$, q, r — простые числа, такие, что $p|q^r+1$. Докажите, что либо $2r|p-1$, либо $p|q^2-1$.

б) Найдите все тройки простых чисел (p, q, r), такие, что $p|q^r + 1$, $q|r^p + 1$, $r|p^q + 1$.

Решение. а) Если $q^r \equiv -1 \pmod p$, то $q^{2r} \equiv 1 \pmod p$. Если T — порядок числа q по модулю p, то $T \mid 2r$, откуда $T \in \{1, 2, r, 2r\}$. Если $T = 1$, то $q \equiv 1 \pmod p$, $1 \equiv q^r \equiv -1 \pmod p$ и $p = 2$ — противоречие. Если $T = r$, то опять $1 \equiv q^r \equiv -1 \pmod p$ и $p = 2$ — противоречие. Значит, либо $T = 2$ и $q^2 \equiv 1 \pmod p$, либо $T = 2r$ и тогда по малой теореме Ферма $2r = T \mid p - 1$, что и требовалось доказать.

б) Ясно, что все числа p, q, r различны. Предположим, что все числа p, q, r больше 2. Согласно п. а), либо $2r \mid p-1$, либо $p \mid q^2-1$. В первом случае получаем, что $0 \equiv p^q+1 \equiv 1+1 = 2 \pmod r$, т.е. $r = 2$ — противоречие. Во втором случае либо $p \mid q-1$, либо $p \mid q+1$. Если $p \mid q-1$, то $0 \equiv q^r+1 \equiv 1+1 = 2 \pmod p$ и $p = 2$ — противоречие. Значит, $p \mid q+1$. Аналогично, $q \mid r+1$ и $r \mid p+1$. Но тогда $p \leqslant q \leqslant r \leqslant p$ и $p = q = r$ — противоречие.

Итак, без ограничения общности $p = 2$. Тогда q и r нечетны. Снова применяя п. а), получаем, что либо $2q \mid r - 1$, либо $r \mid 2^2 - 1 = 3$. В первом случае $r \equiv 1 \pmod q$ и $0 \equiv r^2 + 1 \equiv 1 + 1 = 2 \pmod q$, т.е. $q = 2$, что невозможно. Значит, $r = 3$ и $q = 5$.

Ответ: $(2; 5; 3)$, $(3; 2; 5)$, $(5; 3; 2)$.

20. Найти все пары простых чисел $(p; q)$, таких, что $pq|(5^p - 2^p)(5^q - 2^q)$.

Решение. Пусть $p \mid 5^p - 2^p$. Тогда $0 \equiv 5^p - 2^2 \equiv 5 - 2 = 3 \pmod p$ по малой теореме Ферма, откуда $p = 3$. Значит, $q \mid (5^3 - 2^3)(5^q - 2^q)$ и либо $q = 3$, либо $q \mid 5^3 - 2^3 = 117$ и $q = 13$. Аналогично, если $q = 3$, то $p = 3$ или $p = 17$. Теперь предположим, что $p \neq 3$ и $q \neq 3$. Тогда $p \mid 5^q - 2^q$. Перепишем это в виде $5^q \equiv 2^q \pmod p$ и разделим это сравнение на 2^q. Это можно сделать, т.е. 2^q — делитель единицы по модулю p. Пусть $a = 5/2 \in \mathbb{Z}_p$, тогда $a^q \equiv 1 \pmod p$. Обозначим через T порядок числа a по модулю p. Тогда или $T = 1$, или $T = q$. При $T = 1$ получаем, что $a \equiv 1 \pmod p$ и $5 \equiv 2 \pmod p$, т.е. $p = 3$ — противоречие. При $T = q$ из малой теоремы Ферма получаем, что $q \mid p - 1$. Аналогично, получаем, что $p \mid q - 1$. Но тогда $q < p$ и

$p < q$ — противоречие.

Ответ: $(3;3)$, $(3;13)$, $(13;3)$.

21. Найти все пары простых чисел p, q, таких, что $pq|2^p + 2^q$.

Решение. Заметим, что если $p = 2$, то $q \mid 2 + 2^{q-1}$ и либо $q = 2$, либо $q = 3$. Аналогично, при $q = 2$ получаем, что $p = 2$ или 3. Будем считать, что p и q не равны 2. Пусть $p - 1 = 2^k \cdot n$ и $q = 2^l \cdot m$, где n, m нечетны. Без ограничения общности будем считать, что $k \geqslant l$. Положим $x = 2^n$, тогда согласно малой теореме Ферма, $2^{p-1} \equiv -1 \pmod q$. Значит, порядок числа x по модулю q равен 2^{k+1}, поскольку $x^{2^k} = 2^{p-1} \equiv -1 \pmod q$ и $x^{2^{k+1}} = 2^{2(p-1)} \equiv 1 \pmod q$. Отсюда следует, что $2^{k+1} \mid q - 1 = 2^l \cdot m$, т.е. $k + 1 \leqslant l \leqslant k$ — противоречие.

Ответ: $(2;2)$, $(2;3)$, $(3;2)$.

22. Найти все натуральные n, такие, что наборы простых делителей у чисел n и 2^n+1 совпадают.

Решение. Ясно, что n нечетно. Пусть p — наибольший простой делитель числа n. Тогда $2^p+1 \mid 2^n + 1$. Обозначим через q наибольший простой делитель числа $2^p + 1$. Тогда $q \mid n$ и $q \leqslant p$. С другой стороны, показатель числа 2 по модулю q равен или 1, или 2, или $2p$. В первом случае получаем противоречие, во втором — что $2^2 \equiv 1 \pmod q$ и $q = 3$, а в третьем — что $2p \mid q - 1$ и $q > 2p > p$ — противоречие.

Значит, если у чисел n и $2^n + 1$ совпадают наборы простых делителей, то оба этих числа равны степени тройки. Тогда $2^{3^\alpha} + 1 = 3^\beta$. Если $\alpha \geqslant 2$, то раскладывая левую часть по формуле суммы кубов, последовательно получаем, что числа $2^{3^{\alpha-1}}+1$, $2^{3^{\alpha-2}}+1$, $\ldots$, $2^{3^2}+1$ также являются степенями тройки. Но $2^{3^2} + 1 = 513$ — не степень тройки. Значит, $\alpha = 1$ и $n = 3$ подходит.

Ответ: $n = 3$.

10.3. LTE-лемма

23. Докажите, что

$$\|C_n^k\|_p > \|n\|_p - \frac{k}{p-1}.$$

Решение. Запишем цепочку неравенств:

$$\begin{aligned}\|C_n^k\|_p = \left\|\frac{n(n-1)\ldots(n-k+1)}{k!}\right\|_p \geqslant \|n\|_p - \|k!\|_p = \\ = \|n\|_p - \left(\left[\frac{k}{p}\right] + \left[\frac{k}{p^2}\right] + \left[\frac{k}{p^3}\right] + \ldots\right) > \|n\|_p - \left(\frac{k}{p} + \frac{k}{p^2} + \frac{k}{p^3} + \ldots\right) = \\ = \|n\|_p - \frac{k}{p}\left(1 + \frac{1}{p} + \frac{1}{p^2} + \frac{1}{p^3} + \ldots\right) = \|n\|_p - \frac{k}{p} \cdot \frac{1}{1 - 1/p} = \|n\|_p - \frac{k}{p-1}.\end{aligned}$$

24. Пусть n нечетно и $3^\alpha \| n$. Докажите, что $3^{\alpha+1} \| 2^n + 1$.

Решение. Применим бином Ньютона:

$$2^n + 1 = (-1 + 3)^n + 1 = 3 \cdot C_n^1 - 3^2 \cdot C_n^2 + \ldots \ .$$

Заметим, что $\|3 \cdot C_n^1\|_3 - \alpha + 1$. Докажем, что $\|3^k \cdot C_n^k\|_3 > \alpha + 1$. В самом деле, применяя задачу **23**, получаем:

$$\|3^k \cdot C_n^k\|_3 > k + \|n\|_3 - \frac{k}{2} = \alpha + \frac{k}{2} \geqslant \alpha + 1,$$

что и требовалось доказать.

Теорема 1 (LTE-лемма). *1. Пусть x и y — различные ненулевые целые числа, p — нечетное простое число, не являющееся делителем x и y и такое, что $p \mid x - y$. Тогда для любого натурального n выполнено равенство*

$$\|x^n - y^n\|_p = \|x - y\|_p + \|n\|_p.$$

2. Пусть x и y — различные целые числа, p — нечетное простое число, не являющееся делителем x и y и такое, что $p \mid x+y$. Тогда для любого нечетного натурального n выполнено

$$\|x^n + y^n\|_p = \|x + y\|_p + \|n\|_p.$$

3. Пусть x и y — различные нечетные целые числа и $4 \mid x - y$. Тогда для любого натурального n выполнено

$$\|x^n - y^n\|_2 = \|x - y\|_2 + \|n\|_2.$$

25. Докажите эту теорему.

Доказательство. 1. Пусть $z = x + y$. Тогда

$$x^n - y^n = (y + z)^n - y^n = C_n^1 y^{n-1} z^1 + C_n^2 y^{n-2} z^2 + C_n^3 y^{n-3} z^3 + \dots .$$

Заметим, что

$$\|C_n^1 y^{n-1} z\|_p = \|z\|_p + \|n\|_p.$$

Докажем, что при $k \geqslant 2$ имеет место неравенство

$$\|C_n^k y^{n-k} z^k\|_p > \|z\|_p + \|n\|_p$$

(тогда отсюда будет следовать, что наименьшая степень вхождения p в разность $x^n - y^n$ содержится именно в первом члене бинома Ньютона). Используя неравенство из предыдущей задачи, получаем:

$$\|C_n^k y^{n-k} z^k\|_p = \|C_n^k z^k\|_p = k\|z\|_p + \|C_n^k\|_p > k\|z\|_p + \|n\|_p - \frac{k}{p-1} =$$
$$= (\|n\|_p + \|z\|_p) + (k-1)\|z\|_p - \frac{k}{p-1} \geqslant (\|n\|_p + \|z\|_p) + k - 1 - \frac{k}{2} \geqslant \|n\|_p + \|z\|_p,$$

что и требовалось доказать.

2. Заменим в п.1 число y на число $(-y)$.

3. Здесь нам потребуется немного точнее оценить степени вхождения двойки в биномиальные коэффициенты. Пусть $z = x + y$. Тогда

$$x^n - y^n = (y + z)^n - y^n = C_n^1 y^{n-1} z^1 + C_n^2 y^{n-2} z^2 + C_n^3 y^{n-3} z^3 + \dots .$$

Заметим, что

$$\|C_n^1 y^{n-1} z\|_2 = \|z\|_2 + \|n\|_2.$$

Докажем, что при $k \geqslant 2$ имеет место неравенство

$$\|C_n^k y^{n-k} z^k\|_2 > \|z\|_2 + \|n\|_2$$

(тогда отсюда будет следовать, что наименьшая степень вхождения двойки в выражение $x^n - y^n$ содержится именно в первом члене бинома Ньютона). Используя неравенство из задачи 1, получаем:

$$\|C_n^k y^{n-k} z^k\|_2 = \|C_n^k z^k\|_2 = k\|z\|_2 + \|C_n^k\|_2 > k\|z\|_2 + \|n\|_2 - k =$$
$$= (\|n\|_2 + \|z\|_2) + (k-1)\|z\|_2 - k \geqslant (\|n\|_2 + \|z\|_2) + 2(k-1) - k \geqslant \|n\|_2 + \|z\|_2,$$

что и требовалось доказать. □

26. Пусть натуральные числа x, y, p, n, k таковы, что $x^n + y^n = p^k$. Докажите, что если число $n > 1$ — нечетное, а число p — простое нечетное, то n является степенью числа p с натуральным показателем.

Решение. Без ограничения общности можно считать, что числа x и y не делятся на p (иначе сократим на подходящую степень p; ровно одно из чисел x, y не может быть кратно p). Т.к. $p^k = x^n + y^n \vdots x + y$, то мы находимся в условиях LTE-2. Имеем: $k = \|x^n + y^n\|_p = \|x + y\|_p + \|n\|_p$. Заметим, что $\|x + y\|_p < k$, т.к. $x + y < x^n + y^n = p^k$, поэтому $\|n\|_p = \alpha > 1$. Пусть $n = p^\alpha n_1$. Если $n_1 > 1$, то применим наши рассуждения к уравнению $(x_1)^{n_1} + (y_1)^{n_1} = p^k$, где $x_1 = x^{p^\alpha}$ и $y_1 = y^{p^\alpha}$. Получаем противоречие. Значит, $n_1 = 1$ и $n = p^\alpha$, что и требовалось доказать.

27. Решить уравнение $3^x = 2^x \cdot y + 1$ в натуральных числах.

Решение. Перепишем уравнение в виде $3^x - 1 = 2^x \cdot y$. Заметим, что $x = 1$, $y = 1$ — решение. Далее, если $x \geqslant 2$, то правая часть уравнения делится на 4, а раз так, то $0 \equiv 3^x - 1 \equiv (-1)^x - 1 \pmod 4$, откуда $x = 2n$ — четно.

Запишем уравнение в виде $9^n - 1 = 2^{2n} \cdot y$. Применим LTE-3 (что возможно, т.к. $4 \mid 9 - 1$):

$$2n \leqslant \|9^n - 1\|_2 = \|9 - 1\|_2 + \|n\|_2 = 3 + \|n\|_2.$$

Заметим, что при $\|n\|_2 \leqslant 1$ имеем $2n \leqslant 3 + 1 = 4$, откуда либо $n = 1$, $x = 2$ и $y = 2$, либо $n = 2$, $x = 4$ и $y = 5$. Если же $\|n\|_2 \leqslant 3$, то

$$3 + \|n\|_2 < 2^{\|n\|_2} < 2 \cdot 2^{\|n\|_2} \leqslant 2n,$$

поэтому других решений нет.

28. Найдите все такие натуральные n, что при некоторых взаимно простых x и y и натуральном $k > 1$ выполняется равенство $3^n = x^k + y^k$.

Решение. Заметим, что ни одно из чисел x, y не делится на 3. Значит, их остатки по модулю 3 равны ± 1. Если число k является четным, то тогда $x^k + y^k \equiv 1 + 1 = 2 \neq 0 \pmod 3$ — противоречие. Значит, k нечетно. Применяя результат предыдущей задачи, получаем, что $k = 3^\alpha$.

Положим $u = x^{3^{\alpha-1}}$ и $v = y^{3^{\alpha-1}}$. Тогда $u^3 + v^3 = 3^n$. Раскладывая на множители, получаем, что $u + v = 3^a$ и $u^2 - uv + v^2 = 3^b$, где $a > 1$, $b \geqslant 1$. Тогда

$$3uv = (u + v)^2 - (u^2 - uv + v^2) = 3^{2a} - 3^b.$$

Если $b > 1$, то $uv \vdots 3$ — противоречие. Значит, $b = 1$ и $u^2 - uv + v^2 = 3$. Пусть $u \geqslant v$, тогда

$$3 = u^2 - uv + v^2 \geqslant v^2.$$

Значит, $v = 1$ и $u = 2$, откуда $\alpha = 1$ и $k = 3$.

29. На сколько нулей заканчивается число $4^{5^6} + 6^{5^4}$?

Решение. Заметим, что достаточно вычислить максимальную степень пятерки, на которую делится $4^{5^6} + 6^{5^4}$. Для этого применим LTE-1 и LTE-2:

$$\|4^{5^6} + 1\|_5 = \|4 + 1\|_5 + \|5^6\|_5 = 7 \quad \text{и} \quad \|6^{5^4} - 1\|_5 = \|6 - 1\|_5 + \|5^4\|_5 = 5.$$

Значит, максимальная степень пятерки, на которую делится число $4^{5^6} + 6^{5^4} = (4^{5^6} + 1) + (6^{5^4} - 1)$ равна 5.

Ответ: 5 нулей.

30. Найти максимальную степень k числа 1991, для которой $1991^k \mid 1990^{1991^{1992}} + 1992^{1991^{1990}}$.

Решение. Пусть $a = 1991$. Обозначим через p произвольный простой делитель a. По LTE-1 и LTE-2 имеем

$$\|(a+1)^{a^{a-1}} - 1\|_p = \|(a+1) - 1\|_p + \|a^{a-1}\|_p = a\|a\|_p \quad \text{и}$$
$$\|(a-1)^{a^{a+1}} + 1\|_p = \|(a-1) + 1\|_p + \|a^{a+1}\|_p = (a+2)\|a\|_p.$$

Отсюда следует, что

$$a^a \| (a+1)^{a^{a-1}} - 1 \quad \text{и} \quad a^a | (a-1)^{a^n} + 1.$$

Складывая, получаем, что

$$a^a \| (a-1)^{a^{a+1}} + (a+1)^{a^{a-1}}.$$

Значит, искомая максимальная степень равна $a = 1991$.

31. Докажите, что для любого натурального $a > 2$ найдется такое натуральное $n > 1$, что $a^n - 1$ делится на n^2. Верно ли это утверждение для $a = 2$?

Решение. Обозначим через p простой делитель числа $a - 1$ (т.к. $a > 2$, такой делитель существует). Тогда по LTE-1 имеем

$$\|a^p - 1\|_p = \|a - 1\|_p + \|p\|_p \geqslant 2,$$

т.е. $a^p - 1$ кратно p^2 и можно взять $n = p$.

Если же $a = 2$, то согласно задаче **17** число $2^n - 1$ не делится даже на n.

10.4. Первообразные корни

32. Докажите, что 2 — первообразный корень по модулю 3^n.

Решение. Способ 1. Пусть T — порядок числа 2 по модулю 3^n. Тогда $T = 2t$ четно, т.е. $1 \equiv 2^T \equiv (-1)^T \pmod 3$. Значит, $4^t \equiv 1 \pmod{3^n}$, откуда по LTE-1 имеем $n \leqslant \|4^t - 1\|_3 = \|4 - 1\|_3 + \|t\|_3 = 1 + \|t\|_3$. Значит, $\|t\|_3 \geqslant n - 1$ и $T = 2t \geqslant 2 \cdot 3^{n-1} = \varphi(3^n)$. Получаем, что $T = \varphi(3^n)$, что и требовалось доказать.

Способ 2. Докажем индукцией по n, что показатель числа 2 по модулю 3^n равен $2 \cdot 3^{n-1}$. Пусть T — такой показатель. Ясно, что $2 \mid T$, т.к. $2^T \equiv 1 \pmod 3$, поэтому $T = 2 \cdot 3^\alpha$, т.к. $T \mid \varphi(3^n) = 2 \cdot 3^{n-1}$.

Заметим, что

$$2^{2\cdot 3^\alpha} - 1 = (2^{2\cdot 3^{\alpha-1}} - 1)(2^{4\cdot 3^{\alpha-1}} + 2^{2\cdot 3^{\alpha-1}} + 1).$$

По предположению индукции $\|2^{2\cdot 3^{\alpha-1}} - 1\|_3 = \alpha$. Вторая скобка делится на 3 и дает остаток 3 по модулю 9, т.к. $2 \cdot 3^{\alpha-1} \mid 6 = \varphi(9)$. Значит, произведение этих скобок содержит число 3 в степени $\alpha + 1$. Но $\alpha + 1 \geqslant n$, откуда $\alpha \geqslant n - 1$, что и требовалось доказать.

33. Пусть g — первообразный корень по модулю p. Докажите, что или g, или $g + p$ является первообразным корнем по модулю p^2.

Решение. Пусть T — порядок числа g по модулю p^2. Т.к. g — первообразный корень по модулю p, то $p - 1 \mid T \mid \varphi(p^2) = p(p-1)$. Значит, или $T = p - 1$, или $T = p(p-1)$. Во втором случае g — первообразный корень по модулю p^2. Рассмотрим первый случай. Докажем, что тогда $g + p$ — первообразный корень по модулю p^2. В самом деле, порядок $g + p$ по модулю p^2 равен или $p - 1$, или $p(p-1)$. Во втором случае все доказано, а в первом по биному Ньютона получаем

$$1 \equiv (g+p)^{p-1} \equiv g^{p-1} + pg^{p-2}C_{p-1}^1 + p^2(\ldots) \equiv 1 + pg^{p-2}(p-1) \pmod{p^2}$$

— противоречие.

34. Пусть g — нечетный первообразный корень по модулю простого числа p, причем $g^{p-1}-1$ не делится на p^2. Докажите, что g является первообразным корнем по модулям p^n и $2p^n$.

Решение. Пусть T — порядок числа g по модулю p^n (для модуля $2p^n$ рассуждения дословно совпадают, т.к. $\varphi(2p^n)=\varphi(p^n)$). Т.к. g — первообразный корень по модулю p, то $p-1 \mid T \mid p^{n-1}(p-1)$. Значит, $T=p^k(p-1)$ для некоторого натурального k. Применяя LTE-1, получаем:

$$\|g^T-1\|_p = \|(g^{p-1})^{p^k}-1\|_p = \|g^{p-1}-1\|_p + \|p^k\|_p = 1+k \geqslant n,$$

откуда $k \geqslant n-1$. Значит, $k=n-1$ и $T=\varphi(p^n)$, что и требовалось доказать.

35. Пусть g — первообразный корень по модулю p. Докажите, что существует такое целое t, что число $g+tp$ является первообразным корнем по модулю p^n для любого n.

Решение. Согласно доказательству предыдущей задачи, нам достаточно выбрать такое t, чтобы $p^2 \nmid (g+tp)^{p-1}-1$. Но

$$(g+tp)^{p-1}-1 \equiv (g^{p-1}-1) - tpg^{p-2} \pmod{p^2},$$

поэтому если $p^2 \nmid g^{p-1}-1$, то можно взять $t=0$, а если $p^2 \mid g^{p-1}-1$, то можно взять $t=1$.

Теорема 2. *Первообразные корни существуют лишь по модулям* 2, 4, p^n *и* $2p^n$, *где* p *— нечетное простое число, а* n *— натуральное.*

36. Докажите, что для отличных от указанных в теореме модулей первообразных корней не существует.

Решение. Пусть сначала модуль m равен 2^α. Если g — первообразный корень по модулю m, то $g=1+2t_0$ нечетно, а раз так, то $g^2 \equiv 1+8t_1 \pmod m$, $g^4 \equiv 1+16t_2 \pmod m$, …, $g^{2^{\alpha-2}} = 1+2^\alpha t_{\alpha-2} \equiv 1 \pmod m$. Поэтому g может быть первообразным корнем по модулю m лишь при $\alpha \leqslant 2$.

Пусть теперь $m=2^\alpha p_1^{\alpha_1}\dots p_k^{\alpha_k}$ — разложение модуля m на простые сомножители. Положим $c_i=\varphi(p_i^{k_i})$ и $c_0=1$ при $\alpha=0,1$; $c_0=2$ при $\alpha=2$ и $c_0=2^{\alpha-2}$ при $\alpha>2$. Пусть $h=[c_0,c_1,\dots,c_k]$. Тогда для любого g, взаимно простого с m, имеют место сравнения $g^h \equiv 1 \pmod{2^\alpha}$, $\pmod{p_i^{\alpha_i}}$ (здесь $i=1,\dots,k$). Значит, по китайской теореме об остатках $g^h \equiv 1 \pmod m$. Поэтому g не может быть первообразным корнем, если $h<\varphi(m)$. Но это заведомо так при $\alpha>2$ (тогда $c_0=2^{\alpha-2}<\varphi(2^\alpha)$ и $[c_0,\dots,c_k]<\varphi(2^\alpha)c_1\dots c_k=\varphi(m)$), при $k>1$ (тогда $[c_0,c_1,\dots,c_k]<2^\alpha c_1\dots c_k=\varphi(m)$), и при $k=2$, $\alpha=1$ (тогда $[c_0,c_1]=[2,c_1]=c_1<2c_1=\varphi(m)$).

37. Докажем, что первообразный корень существует для любого простого модуля p. Для этого последовательно докажем следующие утверждения.

а) Над $\mathbb{Z}_p$ (где p — простое) многочлен степени d имеет не более d корней.

б) Пусть ab — порядок числа x по модулю m. Тогда b — порядок числа x^a по модулю m.

в) Пусть d_1, …, d_k — всевозможные порядки всех вычетов по модулю p. Рассмотрим $h=[d_1,\dots,d_k]$. Используя разложение числа h на простые сомножители, докажите существование первообразного корня по модулю p.

Решение. а) Это следствие теоремы Безу: если x_1 — корень многочлена $f(x)$, то $f(x)=(x-x_1)f_1(x)$, причем $\deg f_1 = \deg f - 1$. Продолжая процесс, получим не более $\deg f$ корней многочлена f.

б) Пусть T — показатель числа x^a по модулю m. Тогда ясно, что $T \leqslant b$, т.к. $x^{ab} \equiv 1 \pmod m$. С другой стороны, $(x^a)^T = x^{aT} \equiv 1 \pmod m$, поэтому $ab \mid aT$. Значит, $T=b$, что и требовалось доказать.

в) Пусть $h = q_1^{\alpha_1} \dots q_l^{\alpha_l}$ — разложение h на простые множители. Тогда для каждого q_i найдется $d = aq_i^{\alpha_i}$. Применяя п. б), получаем, что если порядок числа x равен d (такое существует согласно выбору чисел d), то порядок числа x^a равен $q_i^{\alpha_i}$. Перемножим все получающиеся таким образом числа вида x^a и применим китайскую теорему об остатках. Получаем, что существует число x_0 порядка h по модулю h. С другой стороны, все числа 1, 2, ..., $p-1$ в степени h дают 1 по модулю p, поэтому $h \geqslant p-1$ согласно п. а). Окончательно получаем $h = p-1$ и $x_0^{p-1} \equiv 1 \pmod p$, что и требовалось доказать.

Замечание 3. Сразу эта задача следует из задачи **54**.

38. Докажите, что первообразных корней по модулю m ровно $\varphi(\varphi(m))$ штук (если они есть).

Решение. Пусть g — фиксированный первообразный корень по модулю m. Тогда любой другой первообразный корень g' имеет вид g^k для некоторого натурального k. Заметим, что g^k является первообразным корнем тогда и только тогда, когда $(k, \varphi(m)) = 1$. Поэтому первообразных корней в точности $\varphi(\varphi(m))$ штук.

39. Пусть p — простое число. Для каких натуральных k имеет место сравнение

$$\sum_{i=1}^{p-1} i^k \equiv 0 \pmod p?$$

Решение. Пусть g — первообразный корень по модулю p. Если $p-1 \mid k$, то по малой теореме Ферма $\sum\limits_{i=1}^{p-1} i^k \equiv 1 + \ldots + 1 = p-1 \pmod p$. Если же $p-1 \nmid k$, то $g^k \neq 1$ и тогда

$$0 = \sum_{i=1}^{p-1} i^k \equiv \sum_{n=1}^{p-1} g^{kn} = g^k \cdot \frac{g^{k(p-1)} - 1}{g^k - 1} \equiv 0 \pmod p.$$

Ответ: при любых k, не кратных $p-1$.

40. Пусть p — простое число. Докажите, что числа 1, 2, ..., $p-1$ можно расставить по кругу так, чтобы для любых стоящих рядом чисел a, b, c число $b^2 - ac$ не делилось бы на p.

Решение. Запишем все остатки как степени первообразного корня g. Тогда три соседних числа g^α, g^β и g^γ должны удовлетворять условию $p \nmid g^{2\beta} - g^{\alpha+\gamma}$,что равносильно условию $\alpha + \gamma \not\equiv 2\beta \pmod p$. Таким образом, достаточно расположить остатки по модулю p (являющиеся степенями первообразного корня g) так, чтобы никакие три соседних числа не образовывали бы арифметическую прогрессию. Для этого расположим остатки по кругу, разобьем их на пары соседних $(1;2)$, $(3;4)$, ...(все, кроме 0) и поменяем числа в каждой паре местами: 0, 2, 1, 4, 3, ... Легко видеть, что такая расстановка подходит.

41. Докажите, что для любого натурального n найдется такое натуральное m, что $3^n \mid 2^m + 2018$.

Решение. Поскольку 2 является первообразным корнем по модулю 3^n согласно задаче **32**, то для каждого фиксированного n можно найти такое m, чтобы $2^m \equiv -2018 \pmod{3^n}$. Оно и будет искомым.

10.5. Круговые многочлены

42. Докажите, что если p — простое, то $\Phi_p(x) = 1 + x + x^2 + \ldots + x^{p-1}$.

Решение. В самом деле, поскольку p простое, то любое натуральное число, меньшее p, взаимно просто с ним. Поэтому все корни p-й степени из 1 войдут в состав произведения $\Phi_p(x) = \prod\limits_{(k,p)=1} (x - \xi_k)$.

43. Докажите, что $\prod\limits_{d|n} \Phi_d(x) = x^n - 1$. В частности, $\Phi_n(x) \mid x^n - 1$ и $\sum\limits_{d|n} \varphi(d) = n$.

Решение. Заметим, что старшие коэффициенты многочленов слева и справа совпадают, поэтому достаточно доказать, что совпадают множества их корней. Пусть ξ — произвольный корень n-й степени из 1. Тогда рассмотрим наименьшее натуральное d, такое, что $\xi^d = 1$. Ясно, что $d \mid n$ (в противном случае остаток r числа n по модулю d был бы меньше d, и было бы выполнено равенство $\xi^r = 1$). Тогда ξ — корень многочлена $\Phi_d(x)$. Обратно, каждый корень ξ многочлена $\Phi_d(x)$ при $d \mid n$ является корнем степени n из 1, т.к. $(\xi^d)^n = 1$. Таким образом, множества корней многочленов слева и справа совпадают, а раз так, то совпадают и сами многочлены.

При $d = n$ получаем, что $\Phi_n(x) \mid x^n - 1$.

Заметим, что $\deg \Phi_d(x) = \varphi(d)$ для любого натурального d. Приравнивая степени многочленов слева и справа, получаем $\sum\limits_{d|n} \varphi(d) = n$.

44. Докажите, что $\Phi_n(x) \in \mathbb{Z}[x]$.

Решение. Будем вести доказательство индукцией по n. Для $n = 1$ имеем $\Phi_1(x) = x - 1$. Пусть утверждение справедливо для всех $d < n$. Тогда из задачи **43** следует, что $\Phi_n(x) = \dfrac{x^n - 1}{\prod\limits_{d|n, d\neq n} \Phi_d(x)}$ — отношение двух многочленов с целыми коэффициентами. Значит, коэффициенты многочлена $\Phi_n(x)$ рациональны. Но тогда из леммы Гаусса следует, что эти коэффициенты должны быть целыми, что и требовалось доказать.

45. а) Пусть p — произвольное простое число. Докажите, что

$$\Phi_{pn}(x) = \begin{cases} \Phi_n(x^p), & \text{если } p \mid n, \\ \dfrac{\Phi_n(x^p)}{\Phi_n(x)} & \text{если } p \nmid n. \end{cases} \quad \text{и} \quad \Phi_{p^\alpha n}(x) = \begin{cases} \Phi_n(x^{p^\alpha}), & \text{если } p \mid n, \\ \dfrac{\Phi_n(x^{p^\alpha})}{\Phi_n(x^{p^{\alpha-1}})}, & \text{если } p \nmid n. \end{cases}$$

б) Докажите, что при $(n, k) = 1$ имеет место равенство

$$\Phi_n(x^k) = \prod_{d|k} \Phi_{nd}(x).$$

Решение. а) Ясно, что второе равенство следует из первого, поэтому достаточно доказать лишь первое равенство. Пусть $p \mid n$. Заметим, что корни многочленов $\Phi_{pn}(x)$ и $\Phi_n(x^p)$ совпадают: если ξ — корень многочлена $\Phi_n(x^p)$, показатель которого равен T (т.е. наименьшее натуральное t, такое, что $\xi^t = 1$, равно T), то $T \mid np$ и $T \geqslant n$, поэтому $T = n$ или $T = np$. Но если $T = n$, то $\xi^n = (\xi^p)^{n/p} = 1$, поэтому показатель числа ξ^p меньше n, что невозможно. Значит, $T = np$, т.е. ξ является корнем многочлена $\Phi_{np}(x)$. Аналогично доказывается обратное включение. Т.к. эти многочлены являются приведенными, то и сами они также совпадают.

Пусть теперь $p \nmid n$. Докажем равенство $\Phi_n(x^p) = \Phi_{np}(x) \cdot \Phi_n(x)$. Опять пусть ξ — корень многочлена $\Phi_n(x^p)$, показатель которого равен T. Тогда $T \mid np$ и $T \geqslant n$, поэтому $T = n$ или $T = np$. Если $T = n$, то ξ является корнем многочлена $\Phi_n(x)$, а если $T = np$, то ξ является корнем многочлена $\Phi_{np}(x)$. Т.к. все многочлены являются приведенными, и множества корней левой и правой частей совпадают, отсюда следует требуемое.

б) Этот пункт сразу следует из п. а).

46. Докажите, что $\Phi_n(x) \;\Big|\; \dfrac{x^n - 1}{x^k - 1}$ при $k \mid n$ и $k \neq n$.

Решение. Заметим, что

$$x^n - 1 = \prod_{d|n} \Phi_d(x) = \Big(\prod_{d|k} \Phi_d(x)\Big) \cdot \Big(\prod_{d|n, d\nmid k} \Phi_d(x)\Big) = (x^k - 1) \cdot \ldots \cdot \Phi_n(x).$$

47. Пусть p — простой делитель числа $\Phi_n(a)$. Тогда $n = p^\alpha q$, где $\alpha \geqslant 0$ и q — показатель числа a по модулю p.

Решение. Пусть T — показатель числа a по модулю p и $n = p^\alpha q$. Сначала предположим, что $p = 2$. Докажем, что тогда $n = 2^\alpha$. В самом деле, если $2 \mid \Phi_n(a)$, то a нечетно, и если у n есть нечетный делитель d, то по задаче **46** имеем

$$2 \mid \Phi_n(a) \mid \frac{a^n - 1}{a^{n/d} - 1} = a^{(n/d)(d-1)} + a^{(n/d)(d-2)} + \ldots + 1$$

— нечетное число. Противоречие.

Теперь рассмотрим случай $p \geqslant 3$. Тогда по задаче **46**

$$p \mid \Phi_n(a) \mid \frac{a^{p^\alpha q} - 1}{a^T - 1} \equiv \frac{a^q - 1}{a^T - 1} \pmod q.$$

Если $q \neq T$, то по LTE-1 $\|a^q - 1\|_p - \|a^T - 1\|_p + \|q/T\|_p = 0$ — противоречие. Значит, $q = T$ — показатель числа a по модулю p.

48. Докажите, что если числа $\Phi_n(a)$ и $\Phi_m(a)$ не взаимно просты, то $\frac{m}{n}$ является степенью некоторого простого числа (возможно отрицательной).

Решение. По задаче **47** если $p \mid \Phi_n(a)$, то $n = p^\alpha q$, где q — показатель a по модулю p. Аналогично, $m = p^\beta q$. Значит, $\frac{m}{n} = p^{\alpha - \beta}$, что и требовалось доказать.

49. Пусть m и n — целые числа и p — простой делитель $\Phi_n(m)$. Тогда либо $p \mid n$, либо $n \mid p - 1$.

Решение. По задаче **47** имеем $n = p^\alpha q$, где q — показатель числа a по модулю p. Тогда либо $\alpha > 0$ и $p \mid n$, либо $\alpha = 0$ и по малой теореме Ферма $n = q \mid p - 1$.

50. Докажите, что для любого натурального n существует бесконечно много простых чисел p, таких, что $n \mid p - 1$.

Решение. Согласно задаче **4**, у значение многочлена Φ_n в целых точках бесконечно много простых делителей. Если p — один из таких простых делителей, то из задачи **49** следует, что либо $p \mid n$, либо $n \mid p - 1$. Но простых чисел, удовлетворяющих условию $p \mid n$, конечное число. Значит, простых удовлетворяющих условию $n \mid p - 1$, бесконечно много, что и требовалось доказать.

51. Пусть p — простое число. Докажите, что существует такое простое число q, что для любого натурального n число $n^p - p$ не делится на q.

Решение. Рассмотрим число $\Phi_p(p)$. Поскольку $\Phi_p(p) \equiv p + 1 \pmod{p^2}$, у него существует простой делитель q, такой, что $p^2 \nmid q - 1$. Тогда по задаче **49** имеем $p \mid q - 1$.

Предположим, что нашлось такое n, что $n^p \equiv p \pmod q$. Тогда $p^{\frac{q-1}{p}} \equiv n^{q-1} \equiv 1 \pmod q$, откуда $q \mid p^p - 1$ и $q \mid p^{\frac{q-1}{p}} - 1$. Значит, $q \mid p^{\left(\frac{q-1}{p}, p\right)} - 1 = p - 1$, поскольку $\left(\frac{q-1}{p}, p\right) = 1$ (т.к. $p^2 \nmid q - 1$). Получается, что $q \mid p - 1$ и $p \mid q - 1$ — противоречие.

52. Пусть $p_1, \ldots, p_k$ — различные простые числа, большие 3, и $N = 2^{p_1 \cdots p_k} + 1$. Докажите, что у числа N есть хотя бы $2^{2^{k-1}}$ делителей.

Решение. Заметим, что достаточно доказать, что у числа N есть хотя бы $2^{2^{k-1}}$ простых делителей.

Способ 1. Запишем цепочку преобразований:

$$N = 2^{p_1\dots p_k}+1 = \frac{2^{2p_1\dots p_k}-1}{2^{p_1\dots p_k}-1} = \frac{\prod\limits_{d\mid 2p_1\dots p_k}\Phi_d(2)}{\prod\limits_{d\mid p_1\dots p_k}\Phi_d(2)} = \prod_{d\mid p_1\dots p_k}\Phi_{2d}(2).$$

В последнем произведении в точности 2^k множителей. Если мы найдем по одном простому делителю в половине из них и докажем, что они различны, задача будет решена.

Для этого выберем все $d \mid p_1\dots p_k$, содержащие нечетное количество простых множителей p_i. Очевидно, таких чисел будет в точности 2^{k-1}. Рассмотрим теперь простые делители q у чисел $\Phi_{2d}(2)$. Заметим, что если нашелся общий простой делитель у двух таких чисел, то согласно задаче 48 отношение делителей должно быть равно степени простого числа, что невозможно, т.к. это отношение содержит хотя бы два простых числа p_i, p_j.

Способ 2. Упорядочим всевозможные произведения наших простых чисел по возрастанию: $n_1 < n_2 < \ldots < n_{2^{k-1}}$. Заметим, что число N делится на все числа $2^{n_k}+1$, причем по теореме Зигмонди у каждого числа $2^{n_i}+1$ есть простой делитель, которого нет у чисел $2^{n_j}+1$ при $n_j < n_i$. Но это означает, что у числа N будет не менее 2^{k-1} простых делителей — от каждого числа 2^{n_i} у него будет как минимум один простой делитель, что и требовалось доказать.

53. Решить уравнение $\dfrac{x^7-1}{x-1} = y^5-1$ в целых числах.

Решение. Запишем уравнение в виде $\dfrac{x^7-1}{x-1} = (y-1)(y^4+y^3+y^2+y+1)$. Пусть p — произвольный простой делитель левой части. Тогда $p \mid \Phi_7(x)$, поэтому либо $p=7$, либо $p \equiv 1 \pmod 7$. Это означает, что любой делитель левой части либо кратен 7, либо дает остаток 1 при делении на 7. Значит, $y-1 \equiv 0$ или $1 \pmod 7$. Но в первом случае $y \equiv 1 \pmod 7$ и $y^4+y^3+y^2+y+1 \equiv 5 \pmod 7$, а во втором случае $y \equiv 2 \pmod 7$ и $y^4+y^3+y^2+y+1 \equiv 31 \equiv 3 \pmod 7$ — противоречие.

54. Докажите, что мультипликативная группа $\mathbb{K}^\times$ любого конечного поля $\mathbb{K}$ является циклической.

Решение. Пусть поле $\mathbb{K}$ состоит из $n+1$ элемента, тогда его мультипликативная группа (т.е. множество всех элементов, кроме 0) $\mathbb{K}^\times$ состоит из n элементов. По теореме Лагранжа порядок элемента группы делит порядок этой группы, следовательно, для любого элемента $a \in \mathbb{K}^\times$ имеем $a^n = 1$, т.е. все элементы $\mathbb{K}^\times$ являются корнями уравнения $x^n-1=0$. Тогда

$$\prod_{a\in\mathbb{K}^\times}(x-a) = x^n-1 = \prod_{d\mid n}\Phi_d(x).$$

Значит, многочлен $\Phi_n(x)$ имеет ровно $\varphi(n)$ корней в $\mathbb{K}^\times$ (и, значит, хотя бы один). Его корни являются элементами группы $\mathbb{K}^\times$ порядка n, то есть циклическая группа, образованная любым из них, содержит n различных элементов и должна совпадать со всей группой $\mathbb{K}^\times$. Откуда следует цикличность этой группы.

55. Для каждого натурального k рассмотрим операцию f_k, определенную следующим образом:

$$f_k(n) = \Big[\sqrt[k]{\text{наибольший простой делитель числа } (n^{2018k}+1)}\Big].$$

Докажите, что с помощью нескольких таких операций каждое натуральное число можно привести к 1 (в качестве k можно взять любое натуральное число и менять его при необходимости).

Решение. Заметим, что при нечетном k согласно задаче 45, п. б), имеем

$$n^{2018k}+1 = \Phi_4(n^K+1) = \prod_{d\mid K}\Phi_{4d}(n),$$

где $K = 1009k$. Тогда максимальный просто делитель числа $n^K + 1$ в таком случае не превосходит числа $\max(\Phi_{4d}(n))$, где $d \mid K$. Докажем, что можно подобрать число $K = 1009k$ таким образом, чтобы $\Phi_{4d}(n) < (n+1)^{k/2}$ для всех $d \mid K$. Если нам это удастся, то после применения операции f_k мы получим число $f_k(n) < \sqrt{n+1}$, и повторяя аналогичную процедуру, мы в конце концов получим 1, т.к. $\lim\limits_{\ell\to\infty} a_\ell = 1$, где $a_{\ell+1} = \sqrt{a_\ell + 1}$.

Будем искать K в виде $1009p_1p_2\dots p_\ell$, где p_i — идущие по возрастанию простые числа, большие 4036. Заметим, что тогда $\Phi_{4d}(n) < (n+1)^{\varphi(4d)}$. Мы хотим подобрать число ℓ так, чтобы $\varphi(4d) < \frac{k}{2}$ для всех $d \mid K$. Это условие будет заведомо выполнено, если $\frac{\varphi(d)}{K} < \frac{1}{4036}$ для всех $d \mid K$. Ясно, что если $d < K$, то это верно, т.к. $\frac{\varphi(d)}{K} < \frac{d}{K} < \frac{1}{p_1} < \frac{1}{4036}$.

Теперь рассмотрим случай $d = K$. Тогда

$$\frac{\varphi(K)}{K} = \prod_{i=1}^{\ell}\Big(1 - \frac{1}{p_i}\Big).$$

Но правая часть последнего равенства стремится к ∞ при $\ell \to \infty$ (т.к. обратное к ней — частичная сумма гармонического ряда, который расходится). Таким образом, существование нужного нам числа k и вместе с ним искомого процесса, полностью доказано.

10.6. Неприводимость круговых многочленов

56. (критерий Эйзенштейна) Пусть $P(x)$ — приведенный многочлен с целыми коэффициентами, причем все его коэффициенты, кроме старшего, делятся на некоторое простое p, а свободный член не делится на p^2. Докажите, что многочлен $P(x)$ неприводим над $\mathbb{Q}$.

Решение. Пусть $P = f \cdot g$ — разложение многочлена P в произведение двух многочленов ненулевой степени. Запишем

$$P(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0, \quad f(x) = b_kx^k + b_{k-1}x^{k-1} + \ldots + b_1x + b_0,$$
$$g(x) = c_mx^m + c_{m-1}x^{m-1} + \ldots + c_1x + c_0,$$

где $a_i \in \mathbb{Z}$ и b_i, $c_i \in \mathbb{Q}$. По лемме Гаусса можно считать, что b_i, $c_i \in \mathbb{Z}$. Тогда $a_0 = b_0c_0$ и $p \mid a_0$, поэтому либо $p \mid b_0$, либо $p \mid c_0$, но не то и другое одновременно, т.к. $p^2 \nmid a_0$. Без ограничения общности будем считать, что $p \mid b_0$.

Все коэффициенты многочлена f не могут делиться на p, т.к. иначе на p делился бы старший член многочлена P, что невозможно. Пусть i — наименьший индекс, такой, что $p \nmid b_i$. Тогда $a_i = b_ic_0 + b_{i-1}c_1 + \ldots$ также не делится на p, поскольку все слагаемые в правой части, кроме первого, делятся на p. Полученное противоречие доказывает критерий Эйзенштейна.

57. Докажите, что для простого p многочлен $\Phi_p(x)$ неприводим над $\mathbb{Q}$.

Решение. Запишем

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = \frac{\big((x-1)+1\big)^p}{x-1} = \sum_{i=1}^{p} C_p^i(x-1)^i.$$

Применим критерий Эйзенштейна к многочлену $\Phi_p(x-1)$. Каждый его коэффициент C_p^i кратен p, причем свободный член $C_p^1 = p$ не кратен p^2. Поэтому по критерию Эйзенштейна получаем неприводимость многочлена $\Phi_p(x-1)$, а значит, и многочлена $\Phi_p(x)$.

58. Предположим, что $\Phi_n(x) = \prod\limits_{i=1}^{s} Q_i(x)$, где $Q_i \in \mathbb{Q}[x]$ неприводимы и $s > 1$. Пусть также $m = \deg Q_1 \leqslant \deg Q_i$ для всех i.

а) Обозначим через $x_1, \ldots, x_m$ (комплексные) корни многочлена Q_1. Докажите, что для любого k многочлен $\widetilde{Q}_k(x) = \prod_{i=1}^{m}(x - x_i^k)$ имеет целые коэффициенты.

б) Докажите, что $\Phi_n = \prod_{k:(k,n)=1} \widetilde{Q}_k$.

в) Докажите, что существует такое k, что $\widetilde{Q}_k \neq Q_1$ и при этом сравнение $p \equiv k \pmod n$ имеет бесконечно много решений в простых числах.

г) Завершите доказательство теоремы о неприводимости круговых многочленов.

Замечание 4. Данное доказательство следует рассуждениям А. Я. Канель-Белова из статьи «О круговых многочленах», Математическое Просвещение, сер. 3, вып. 8 (2004), с. 181–184.

Решение. а) Заметим, что коэффициенты многочлена $\widetilde{Q}_k$ являются симметрическими функциями от $x_1, \ldots, x_m$. Поэтому эти коэффициенты полиномиально выражаются через элементарные симметрические многочлены от $x_1, \ldots, x_m$. Эти элементарные симметрические многочлены являются целыми числами по теореме Виета, т.к. с точностью до знака они равны коэффициентам многочлена Q_1. Значит, коэффициенты многочлена $\widetilde{Q}_k$ также будут целыми числами, что и требовалось доказать.

б) Заметим, что числа $x_1, \ldots, x_m$ являются примитивными корнями n-й степени из единицы. Тогда если $(k, n) = 1$, то числа x_i^k также будут являться примитивными корнями n-й степени из единицы. Значит, число x_1^k будет корнем некоторого многочлена Q_i. Но поскольку Q_i неприводим и $\deg Q_i \geqslant m = \deg \widetilde{Q}_k$, то $Q_i = \widetilde{Q}_k$. Обратно, взяв любой многочлен Q_i, найдем такое r, что x_1^r будет его корнем. Тогда Q_i совпадает с $\widetilde{Q}_r$.

в) Рассмотрим множество таких остатков k по модулю n, что $\widetilde{Q}_k = Q_1 = \widetilde{Q}_1$. Это множество является подгруппой $G \subset \mathbb{Z}_n^*$. При этом в силу приводимости многочлена Φ_n эта подгруппа не совпадает со всем $\mathbb{Z}_n^*$. По задаче **7** найдется такое k_0, что $\widetilde{Q}_{k_0} \neq Q_1$, причем для бесконечно многих простых p выполняется сравнение $p \equiv k_0 \pmod n$, что и требовалось доказать.

г) Рассмотрим редукции многочленов $\widetilde{Q}_{k_0}$ и Q_1 по модулю достаточно большого простого p, удовлетворяющего сравнению $p \equiv k_0 \pmod n$. Тогда с одной стороны все корни редукции $\widetilde{Q}_k$ совпадают с корнями редукции Q_1, а потому редукции многочленов $\widetilde{Q}_k$ и Q_1 по модулю p должны совпасть. С другой стороны, $\widetilde{Q}_k \neq Q_1$, поэтому при достаточно больших p их редукции должны быть различны. Полученное противоречие доказывает теорему о неприводимости круговых многочленов.

10.7. Теорема Зигмонди

59. Пусть $n = p^\alpha q$, где $p \nmid q$. Докажите, что $\alpha > 0$. Отсюда следует, что p — *наибольший простой делитель* числа n.

Решение. По задаче **46** $p \mid \Phi_n(a) \;\Big|\; \frac{a^n-1}{a^k-1}$. По LTE-1

$$\|a^n - 1\|_p = \|a^k - 1\|_p + \left\|\frac{n}{k}\right\|_p \geqslant 1,$$

откуда $p \;\Big|\; \frac{n}{k}$ и $p \mid n$, что и требовалось доказать.

60. Докажите, что если $p = 2$, то $n = 2$ и $a + 1$ — степень двойки.

Решение. Согласно задаче **59**, 2 — это наибольший делитель n, значит, $n = 2^\alpha$. Но тогда a нечетно и по задаче **45**

$$\Phi_n(a) = \Phi_{2^\alpha}(a) = \Phi_2(a^{2^{\alpha-1}}) = \Phi_n(a^{n/2}) = a^{n/2} + 1.$$

При $n > 2$ имеем $a^{n/2} + 1 \equiv 2 \pmod 4$ — противоречие. Значит, $n = 2$ и $a + 1$ — степень двойки, что и требовалось доказать.

61. Докажите, что если $p > 2$, то $\|\Phi_n(a)\|_p = 1$.

Решение. Ясно, что $\|\Phi_n(a)\|_p \geqslant 1$. С другой стороны, по задаче **46** $\Phi_n(a) \;\Big|\; \frac{a^n-1}{a^{n/p}-1}$. Заметим, что по задаче **47** $p \mid a^q - 1 \mid a^{n/p} - 1$, поэтому по LTE-1

$$\left\| \frac{a^n - 1}{a^{n/p} - 1} \right\|_p = \|a^n - 1\|_p - \|a^{n/p} - 1\|_p = \|p\|_p = 1.$$

Значит, $\|\Phi_n(a)\|_p \leqslant 1$, откуда получаем требуемое.

62. Пусть $n = p^\alpha q$, где $p \nmid q$.

а) Докажите, что $\Phi_n(a) > p$ при $\alpha > 1$.

б) Докажите, что $\Phi_n(a) > p$ при $\alpha = 1$ и $a > 2$.

в) Докажите, что $\Phi_n(a) > p$ при $\alpha = 1$ и $a = 2$, за исключением случая $n = 6$.

Решение. а) Имеем:

$$\Phi_n(a) = \Phi_{p^\alpha q}(a) = \Phi_{p^{\alpha-1}q}(a^p) \geqslant a^p - 1 \geqslant 2^p - 1 > p,$$

что и требовалось доказать.

б) Имеем:

$$\Phi_n(a) \geqslant (a-1)^{\varphi(n)} \geqslant 2^{\varphi(n)} \geqslant 2^{p-1} \geqslant p,$$

что и требовалось доказать.

в) Имеем:

$$\Phi_n(2) = \frac{\Phi_q(2^p)}{\Phi_q(2)} \geqslant \frac{2^p - 1}{3} > p$$

при $p \geqslant 5$.

При $p = 3$ имеем $n = 3q$, причем $q = 1$ или 2. Если $n = 3$, то $\Phi_3(2) = 2^2 + 2 + 1 = 7 > 3$. Если $n = 6$, то $\Phi_6(2) = 2^2 - 2 + 1 = 3$, что дает второе исключение в теореме Зигмонди.

Тем самым п.1 теоремы Зигмонди в случае $b = 1$ полностью доказан.

63. Докажите п.1 теоремы Зигмонди для произвольных a и b.

Решение. Рассмотрим однородные круговые многочлены $\Phi_n(a, b) = b^{\varphi(n)} \cdot \Phi_n(a/b)$. Тогда все факты и доказательства из задач **59**–**61** дословно переносятся на однородные круговые многочлены (достаточно рассмотреть остаток a/b по модулю p). Для задачи **62** необходимо немного подправить оценки для значений однородных круговых многочленов $\Phi_n(a, b)$.

а) При $\alpha > 1$ имеем

$$\Phi_n(a, b) = \Phi_{p^{\alpha-1}q}(a^p, b^p) \geqslant a^p - b^p \geqslant (b+1)^p - b^p > bp \geqslant p.$$

б) При $\alpha = 1$ и $a - b > 1$ имеем

$$\Phi_n(a, b) \geqslant (a-b)^{\varphi(n)} \geqslant 2^{p-1} \geqslant p.$$

в) При $\alpha = 1$ и $a - b = 1$ имеем

$$\Phi_n(a, b) = \frac{\Phi_q(a^p, b^p)}{\Phi_q(a, b)} \geqslant \left(\frac{a^p - b^p}{a + b}\right)^{\varphi(q)} \geqslant \frac{(b+1)^p - b^p}{2b+1} \geqslant \frac{(2^p - 1)b}{3} \geqslant \frac{2^p - 1}{3} > p$$

при $p \geqslant 5$. При $p = 3$ неравенство $\Phi_n(a, b) > p$ заведомо выполнено при $b \geqslant 2$, поэтому исключением является уже разобранный в задаче **62** случай $b = 1$.

64. Докажите п.2 теоремы Зигмонди.

Решение. По п.1 теоремы Зигмонди у числа $a^{2n}-b^{2n}$ существует простой делитель p, которого нет у чисел a^k-b^k для всех $k<2n$, кроме случаев $n=1$ и $a+b$ равного степени двойки и $n=3$, $a=2$ и $b=1$. В частности, p не делит $a^{2k}-b^{2k}=(a^k-b^k)(a^k+b^k)$ для всех $k<n$.

Таким образом, достаточно проверить случай $n=1$ и $a+b$ равном степени двойки. Заметим, что числа a и b нечетны, поэтому $a^2+b^2\equiv 2 \pmod 4$. Кроме того, $a^2+b^2>2$. Таким образом, у числа a^2+b^2 если нечетный простой делитель, которого нет у числа $a+b$. Это завершает доказательство теоремы Зигмонди.

65. Найти все решения уравнения

$$a^n-1=(a^p-1)(a^q-1)(a^r-1)$$

в натуральных числах.

Решение. Если $a\geqslant 3$ и $n\geqslant 3$, то по теореме Зигмонди у числа a^n-1 есть простой делитель, которого нет у чисел a^p-1, a^q-1 и a^r-1. Осталось разобрать случаи $a=1$, $a=2$ и $n=1$, $n=2$, $n=6$. Простым перебором легко убедиться, что подходят $a=1$ и любые n, p, q, r, а также $a=2$, $n=6$, $p=3$, $q=r=2$.

Ответ: $a=1$ и любые n, p, q, r, а также $a=2$, $n=6$, $p=3$, $q=r=2$.

66. Найти все натуральных числа a, m, n, такие, что $a^m+1 \mid (a+1)^n$.

Решение. Заметим, что $a=2$, $m=3$ и $n\geqslant 2$ подходят. Для $a>1$ и $m\geqslant 2$, отличных от пары $(2,3)$, решений нет по теореме Зигмонди (т.к. число a^m+1 содержит простой делитель, которого нет у числа $a+1$). Случаи $a=1$ или $m=1$, очевидно, дают решения.

Ответ: $a=1$, m, n любые; a любое, $m=1$, n любое; $a=2$, $m=3$, n любое.

67. Найти все такие натуральны числа x, p, n, r, такие, что p простое, n, $r>1$ и $x^r-1=p^n$.

Решение. По теореме Зигмонди решениями могут быть лишь $x=2$, $r=6$ или $r=2$ и $x+1=2^k$. Первый случай не дает решений, а во втором $p=2$ и

$$2^n=x^2-1=(x-1)(x+1)=2^k(x-1),$$

откуда $x-1=2^{n-k}$. Но тогда $x+1$ и $x-1$ — различающиеся на 2 степени двойки, поэтому $x=3$ и $n=3$.

Ответ: $x=3$, $p=2$, $n=3$, $r=1$.

68. Найти все натуральные решения уравнения $p^x-y^p=1$, где p — простое.

Решение. Перепишем уравнение в виде $p^x=y^p+1$. При $y=1$ получаем решение $p=2$ и $x=1$; при $y=2$ и $p=3$ получаем решение $x=2$. При всех остальных y и p по теореме Зигмонди у числа y^p+1 есть простой делитель, которого нет у числа $y+1$. Поскольку $y+1 \mid y^p+1$ (т.к. p нечетно), у числа y^p+1 есть не менее двух различных простых делителей, и у нашего уравнения нет решений.

Ответ: $x=1$, $y=1$, $p=2$ и $x=y=2$, $p=3$.

69. Решить уравнение $5^x-3^y=z^2$ в натуральных числах.

Решение. Рассмотрим уравнение по модулю 3. Т.к. $3\nmid z$, то $z^2\equiv 1 \pmod 3$, откуда $x=2w$ — четное. Значит,

$$3^y=5^{2w}-z^2=(5^w-z)(5^w+z).$$

Поскольку $(5^w-z,5^w+z)=1$, то $5^w-z=1$ и $5^w+z=3^y$, причем $y\geqslant 2$. Складывая эти равенства, находим $2\cdot 5^w=3^y+1$. Для $y=2$ получаем $w=1$, откуда находим решение $x=y=2$ и $z=4$. Для $y\geqslant 3$ по теореме Зигмонди у числа 3^y+1 есть простой делитель, которого нет у числа $3^2+1=10$. Но тогда число $2\cdot 5^w$ должно делиться на это простое, что невозможно. Таким образом, других решений нет.

Ответ: $x = y = 2$, $z = 4$.

70. Найти все натуральные решения уравнения $p^a - 1 = 2^n(p-1)$, где p — простое.

Решение. Очевидно, что p нечетно. Докажем, что число a должно быть простым. Пусть $a = uv$, где u, $v > 1$. Тогда по теореме Зигмонди числа $p^u - 1$ есть простой делитель, которого нет у $p-1$. С другой стороны, $p^u - 1 \mid p^a - 1 = 2^n(p-1)$, поэтому этот простой делитель может быть только двойкой. Но $2 \mid p - 1$ — противоречие.

Итак, a простое. При $a = 2$ получаем $p = 2^n - 1$, т.е. p — простое число Мерсенна. Если же a нечетно, то по теореме Зигмонди число $p^a - 1 = 2^n(p-1)$ должно иметь простой делитель, которого нет числа $p - 1$. Но таких простых не существует — противоречие.

Ответ: $a = 2$, $p = M_n$ — простое число Мерсенна.

71. Решить уравнение

$$(a+1)(a^2+a+1)\dots(a^n+a^{n-1}+\dots+a+1) = a^m + a^{m-1} + \dots + a + 1$$

в натуральных числах.

Решение. Заметим, что $m = n = 1$ дает решение. Также при $a = 1$ есть решение $m = (n+1)!$. При $m > n > 1$ и $a > 1$ домножим обе части уравнения на $(a-1)^n$. Получим уравнение

$$(a^2-1)(a^3-1)\dots(a^{n+1}-1) = (a^{m+1}-1)(a-1)^{n-1}.$$

По теореме Зигмонди единственное решение здесь возможно при $a = 2$ и $m + 1 = 6$, поскольку в противном случае у числа $a^{m+1} - 1$ есть простой делитель, которого нет у $a^2 - 1, \dots, a^{n+1} - 1$. Однако при $a = 2$ и $m = 5$ целого n не существует.

Ответ: $m = n = 1$, a любое и $a = 1$, $m = (n+1)!$, n любое.

10.8. Разные задачи

72. Докажите, что существует такое натуральное n, что $8^n + 2018$ делится на 5^{2018}.

Решение. Заметим, что 8 является первообразным корнем по модулю 5^n для любого натурального n. В самом деле, пусть T — порядок числа 8 по модулю 5^n. Тогда $8^T \equiv 1 \pmod 5$, поэтому $T = 4t$. Тогда по LTE-1 получаем:

$$n \leqslant \|8^T - 1\|_5 = \|4096^t - 1\|_5 = \|4096 - 1\|_5 + \|t\|_5 = 1 + \|t\|_5,$$

откуда $t \geqslant 5^{n-1}$ и $T \geqslant 4 \cdot 5^{n-1} = \varphi(5^n)$. Значит, $T = \varphi(5^n)$.

Теперь выберем такое n, чтобы $8^n \equiv -2018 \pmod{5^{2018}}$. Оно и будет искомым.

73. Существует ли такое натуральное N, что у числа N в точности 2019 простых делителей и $N \mid 2^N + 1$?

Решение. Докажем, что для любого натурального m существует такое число N, у которого в точности m простых делителей и которое делит $2^N + 1$. Будем вести доказательство индукцией по m. При $m = 1$ можно взять $N = 3$. Пусть мы построили число $N = p_1^{\alpha_1} \dots p_m^{\alpha_m}$, имеющее в точности m простых делителей и делящее $2^N + 1$. Ясно, что все p_i нечетны. Пусть

$$\|2^N + 1\|_{p_i} = \beta_i \geqslant \alpha_i,$$

тогда $p_1^{\beta_1} \dots p_m^{\beta_m} \| 2^N + 1$. Согласно LTE-2, для любого натурального l имеет место равенство $\|2^{Np_1^l} + 1\|_{p_1} = \|2^N + 1\|_{p_1} + \|p_1^l\|_{p_1} = \beta_1 + l$, поэтому $p_1^{\beta_1 + l} \dots p_m^{\beta_m} \| 2^{Np_1^l} + 1$. Выбирая l достаточно

большим, можно добиться, чтобы $2^{Np_1^l}+1 > p_1^{\beta_1+l}\dots p_m^{\beta_m}$. Тогда у числа $2^{Np_1^l}+1$ существует простой делитель p_{m+1}, отличный от $p_1, \dots, p_m$. Тогда

$$Np_1^l p_{m+1} \mid 2^{Np_1^l}+1 \mid 2^{Np_1^l p_{k+1}}+1,$$

и можно взять $N' = Np_1^l p_{m+1}$. Тем самым индукционный переход доказан.

74. Пусть N — натуральное число, заканчивающееся на 25, а m — произвольное натуральное число. Докажите, что существует такое натуральное n, что у m последних цифр в записи чисел N и 5^n совпадают четности, а у $(m+1)$-ых цифр четности различны.

Решение. Будем вести доказательство индукцией по m. Для $m = 1$ и 2 утверждение очевидно. Для проведения шага индукции достаточно показать, что при $n \geqslant m \geqslant 2$ правые m цифр у чисел 5^n и $5^{n+2^{m-2}}$ совпадают по четности, но $(m+1)$-е цифры имеют разную четность. Применяя LTE-3, имеем $\|5^{2^{m-2}}-1\|_2 = \|5-1\|_2 + \|2^{m-2}\|_2 = 2+(m-2) = m$. Значит, разность $5^{n+2^{m-2}} - 5^n$ делится на 10^m, но не делится на $2\cdot 10^m$. Тем самым утверждение доказано.

75. Пусть p — простое число и a, n — натуральные числа. Докажите, что если $2^p + 3^p = a^n$, то $n = 1$.

Решение. При $p = 2$ утверждение очевидно. Пусть $p > 2$ — нечетное простое число. Заметим, что тогда $5 \mid a$. Применим LTE-2:

$$n \leqslant \|2^p+3^p\|_5 = \|2+3\|_5 + \|p\|_5 \leqslant 2,$$

причем равенство может достигаться лишь при $p = 5$. Но при $p = 5$ прямой проверкой убеждаемся, что $n = 1$.

76. Докажите, что разность $3^n - 2^n$ не делится на n ни для какого натурального n.

Решение. Предположим противное: пусть $n \mid 3^n - 2^n$. Рассмотрим наименьший простой делитель p числа n. Ясно, что $p \neq 2, 3$. Тогда $3^n \equiv 2^n \pmod p$ и $a^n \equiv 1 \pmod p$, где $a \equiv 3/2 \pmod p$. Обозначим через T порядок числа a по модулю p. Тогда по малой теореме Ферма $T \mid p-1$ и $T < p$. С другой стороны, $T \mid n$. В результате мы нашли делитель числа n, меньший p, поэтому $T = 1$ и $3 \equiv 2 \pmod p$ — противоречие.

77. Докажите, что если $3^n - 2^n = p^a$ для некоторых натуральных n, a и простого p, то тогда n — простое.

Решение. Предположим, что $n = qm$, где q — простой делитель n. Тогда $3^m - 2^m = p^b$ для некоторого целого неотрицательного b. Применяя LTE-1, получаем:

$$a = \|(3^m)^q - (2^m)^q\|_p = \|3^m-2^m\|_p + \|q\|_p = b,$$

откуда получаем, что $3^m - 2^m \geqslant p^b = p^a = (3^m-2^m)(\dots)$, что возможно, только если $m = 1$.

78. Докажите, что существует бесконечно много составных чисел n, таких, что выполнено следующее свойство: если $n \mid a^n - 1$, то $n^2 \mid a^n - 1$ для любого натурального a.

Решение. Во-первых, заметим, что если $n = p$ — простое, то указанное свойство выполнено. В самом деле, из малой теоремы Ферма следует, что $a^p \equiv a \equiv 1 \pmod p$, поэтому по LTE-1 имеем $\|a^p-1\|_p = \|a-1\|_p + \|p\|_p \geqslant 1+1 = 2$. Теперь рассмотрим такие натуральные n, которые содержат каждое простое число в своем разложении на простые сомножители в степени 1. Пусть $n = qk$, где q — простое. Применяя рассуждения, описанные выше, к числу $b = a^k$, получаем, что $q^2 \mid b^q - 1 = a^n - 1$. Значит, $n^2 \mid a^n - 1$, что и требовалось доказать.

79. Найдите все натуральные $n > 1$, такие, что число $\dfrac{2^n+1}{n^2}$ является целым.

Решение. Пусть p — наименьший простой делитель числа n. Тогда $p \geqslant 3$ и $2^n \equiv -1 \pmod p$. Получаем, что $2^{2n} \equiv 1 \pmod p$. Обозначим через T порядок числа 2 по модулю p. Тогда $T \mid q-1$ и $T \mid 2n$. Значит, $T < q$ и потому либо $T = 1$, либо $T = 2$ (иначе в T найдется простой делитель n, меньший p). При $T = 1$ получаем, что $2 \equiv 1 \pmod p$ — противоречие. Поэтому $T = 2$ и $2^2 \equiv 1 \pmod p$. Значит, $p = 3$.

Теперь применим LTE-2:

$$1 + \|n\|_3 = \|2 + 1\|_3 + \|n\|_3 = \|2^n + 1\|_3 \geqslant \|n^2\|_3 = 2\|n\|_3,$$

откуда следует, что $\|n\|_3 = 1$.

Пусть $n = 3m$. Если $m = 1$, то $n = 3$ — ответ. В противном случае $m > 3$ — нечетно, и пусть q — наименьший простой делитель m. Тогда $q > 3$. Получаем: $2^{3m} \equiv -1 \pmod q$ и $2^{6m} \equiv 1 \pmod q$. Пусть t — порядок двойки по модулю q. Тогда $t \mid q-1$ и $t \mid 6m$. Но $t < q$, поэтому $(t, m) = 1$, значит, $t \mid 6$. Если $t = 3$, то $2^{3m} \equiv 1 \pmod q$ — противоречие. При $t = 1$ получаем, что $2 \equiv 1 \pmod q$ — противоречие. Если $t = 2$, то $2^2 \equiv 1 \pmod q$ и $q = 3$ — противоречие. Значит, $t = 6$. Тогда $2^6 \equiv 1 \pmod q$ и $q = 7$.

Получаем, что $7 \mid 2^n + 1$. Однако, перебрав все остатки n по модулю 6, легко убедиться, что это невозможно. Таким образом, мы получаем противоречие.

Ответ: $n = 3$.

80. Пусть b, m, n — натуральные числа, такие, что $b > 1$ и $m \neq n$. Докажите, что если $b^m - 1$ и $b^n - 1$ имеют одинаковый набор простых делителей, то $b + 1$ является степенью двойки.

Решение. Прежде всего заметим, что, применяя алгоритм Евклида для степеней, условие можно переписать так: числа $b^m - 1$ и $b^{(n,m)} - 1$ имеют одинаковые наборы простых делителей. Далее, сделаем замену $(n, m) = d$, $m = dk$, $b^d = a$. Тогда условие перепишется в такое виде: $a^k - 1$ и $a - 1$ имеют одинаковые наборы простых делителей.

Заметим, что если мы докажем, что $a+1$ является степенью двойки, то тогда число d должно быть нечетным (иначе $4 \nmid b^d + 1 = a + 1$), поэтому $b + 1 \mid b^d + 1 = a + 1$ и $b + 1$ также будет степенью двойки.

Предположим, что число k делится на нечетное простое p и $\|k\|_p = \beta$. Тогда у числа $X = \dfrac{a^{p^\beta} - 1}{a - 1}$ и у $a-1$ также одинаковые наборы простых делителей (т.к. $a^{p^\beta} - 1 \mid a^k - 1$). Пусть $q \mid X$ и $q \mid a - 1$. Тогда $a \equiv 1 \pmod q$ и $X \equiv p^\beta \equiv 0 \pmod q$. Значит, $q = p$ и X является степенью числа p. По LTE-1 имеем $\|X\|_p = \|a^{p^\beta} - 1\|_p - \|a - 1\|_p = \|p^\beta\|_p = \beta$ и $X = p^\beta$, что невозможно при $a > 1$.

Значит, число k является степенью двойки. Но тогда $a^2 - 1$ и $a - 1$ имеют одинаковые наборы простых делителей, а значит, и $a + 1$ и $a - 1$ имеют одинаковые наборы простых делителей. Т.к. $(a - 1, a + 1) = 2$ (эти числа не могут быть взаимно просты), то $a + 1$ является степенью двойки. Как мы уже поняли, отсюда следует, что $b + 1$ также является степенью двойки, что и требовалось доказать.

81. Докажите, что все числа

$$10001, \quad 100010001, \quad 1000100010001, \quad \ldots$$

являются составными.

Решение. Необходимо доказать, что число $a_n = 1 + 10^4 + 10^8 + \ldots + 10^{4n} = \frac{10^{4(n+1)}-1}{10^4-1}$ является составным. При $n = 0$ имеем $10001 = 137 \cdot 73$. Далее, ясно, что если $m + 1 \mid n + 1$, то $a_m \mid a_n$. Поэтом достаточно доказать утверждение при $n+1 = p$ — простом. В таком случае по задаче **45** имеем $\Phi_p(10^4) = \Phi_p(10) \cdot \Phi_{4p}(10)$, т.е. число $\Phi_p(10^4)$ составное, что и требовалось доказать.

82. Найти все тройки (p, x, y), состоящие из простого числа p и двух натуральных чисел x и y, таких, что $x^{p-1} + y$ и $x + y^{p-1}$ являются степенями числа p.

Решение. Пусть $p = 2$. Тогда $x+y = p^k$ для некоторого натурального k, поэтому x может быть любым натуральным числом, меньшим p^k, а $y = p^k - x$.

Пусть теперь $p > 2$. Заметим, что $x \neq y$, иначе $x + x^{p-1} = x(1 + x^{p-2})$ не может быть точной степенью, поскольку множители x и $1 + x^{p-2}$ взаимно просты. Кроме того, ясно, что $p \nmid x$, y (в противном случае степень вхождения p в одно из слагаемых меньше, чем в другое). Будем считать, что $x < y$. Тогда $x^{p-1} + y = p^a$ и $x + y^{p-1} = p^b$, причем $a < b$. Домножая первое равенство на x, второе на y и вычитая их, получаем, что $p^a \| y^p - x^p$. Далее, по малой теореме Ферма $y^p - x^p \equiv y - x \equiv 0 \pmod p$, поэтому по LTE-1 $a = \|y^p - x^p\|_p = \|y - x\|_p + \|p\|_p$, а значит, $p^{a-1} \| y - x$. Положим $y - x = p^{a-1}q$.

Подставляя $y = x + p^{a-1}q$ в равенство $x^{p-1} + y = p^a$, получаем $x^{p-1} + x = p^a(p - q)$, откуда $x \mid p - q$ (т.к. $p \nmid x$). Далее, подставляя $y = p^a - x^{p-1}$ в равенство $x + y^{p-1} = p^b$, получаем: $0 \equiv x + (p^a - x^{p-1})^{p-1} \equiv x + x^{(p-1)^2} \equiv x + 1 \pmod p$, откуда $x \equiv -1 \pmod p$.

Итого с одной стороны, $x \mid p - q$ и $x \leqslant p - q \leqslant p - 1$, а с другой, $p \mid x + 1$ и $x + 1 \geqslant p$. Значит, $x = p - 1$, $q = 1$ и $y = p - 1 + p^{a-1}$. Подставляя это в равенство $x^{p-1} + y = p^a$, получаем $(p-1)^{p-1} + (p-1) + p^{a-1} = p^a$, откуда $(p-1)^{p-2} + 1 = p^{a-1}$. Применяя LTE-2 к этому равенству, получаем $a - 1 = \|(p-1)^{p-2} + 1\|_p = \|(p-1) + 1\|_p + \|p - 2\|_p = 1$, откуда $a = 2$. Наконец, из равенства $(p-1)^{p-2} + 1 = p$ получаем, что $p = 3$.

Ответ: $(3; 2; 5)$, $(3; 5; 2)$, $(2; n; 2^k - n)$, где $1 \leqslant n \leqslant 2^k - 1$.

83. Пусть m — нечетное натуральное число, $m > 3$. Найти наименьшее натуральное n, такое, что $2^{2019} \mid m^n - 1$.

Решение. Заметим, что числа $m - 1$ и $m + 1$ четны и имеют НОД, равный 2, поэтому условие равносильно тому, что $2^{2020} \mid m^{2n} - 1$. Тогда $4 \mid m^2 - 1$, и по LTE-3 имеем $2020 \leqslant \|m^{2n} - 1\|_2 = \|m^2 - 1\|_2 + \|n\|_2 = a + \|n\|_2$. Значит, $\|n\|_2 \geqslant 2020 - a$. Поэтому при $a \leqslant 2020$ наименьшее число $n = 2^{2020-a}$, и при $a > 2020$ можно взять $n = 1$.

Ответ: если $a = \|m^2 - 1\|_2$, то $n = 2^{2020-a}$ при $a \leqslant 2020$ и $n = 1$ при $a > 2020$.

84. Докажите, что существует бесконечно много натуральных n, таких, что все простые делители числа $n^2 + 1$ меньше $\sqrt{n}$.

Решение. Будем искать $n = a^k$ для подходящих k. Заметим, что по задаче **45** имеем

$$n^2 + 1 = \Phi_4(a^k) = \prod_{d \mid k} \Phi_{4d}(a).$$

Теперь будем искать $k = p_1^{\alpha_1} \dots p_m^{\alpha_m}$, где p_i — простые, не равные 3. Достаточно найти такое k, что $\varphi(4d) < \frac{k}{2}$ при всех $d \mid k$: в таком случае степень $\varphi(4d)$ каждого множителя $\Phi_{4d}(a)$ как многочлена от a будет меньше $2^{k/2} = \sqrt{n}$, а значит, при достаточно больших a простые множители чисел $\Phi_{4d}(a)$ тоже будут меньше $\sqrt{n}$. Для этого достаточно найти такие k, что $\varphi(d) < ck$, где $c = \frac{1}{4}$ и $d \mid k$.

Будем искать k в виде $p_1 \dots p_m$, где числа p_i — последовательные простые числа, большие c^{-1}. Тогда при $d < k$ имеем $\varphi(d) < d < ck$. Если же $d = k$, то

$$\frac{\varphi(k)}{k} = \prod_{i=1}^{m} \Big(1 - \frac{1}{p_i}\Big).$$

Но при $m \to \infty$ данное произведение стремится к 0 (т.к. обратное к нему — частичная сумма гармонического ряда, который расходится). Поэтому при достаточно большом m будет выполнено неравенство $\frac{\varphi(k)}{k} < c$. Следовательно, взяв $n = 2^k$, мы получим бесконечное количество искомых натуральных n, что и требовалось.

85. Найти все натуральные числа n и p, такие, что p — простое, $n \leqslant 2p$ и $n^{p-1} \mid (p-1)^n + 1$.

Решение. Сначала разберем тривиальные случаи. Если $n = 1$, то p — любое простое число. Если $p = 2$, то $n = 2$. Если $p \geqslant 3$, то n нечетно. Поэтому далее будем считать, что $n \geqslant 3$ — нечетно и $p \geqslant 3$.

Обозначим через q наименьший простой делитель числа n. Тогда

$$(p-1)^n \equiv -1 \pmod{q} \quad \text{и} \quad (p-1)^{2n} \equiv 1 \pmod{q}.$$

Пусть T — порядок числа $p-1$ по модулю q. Тогда $T \mid q-1$ и $T \mid 2n$. Получаем, что $T < q$, поэтому $(T, n) = 1$ и $T \mid 2$. Если $T = 1$, то $-1 \equiv p-1 \equiv 1 \pmod{q}$ и $q = 2$ — противоречие. Поэтому $T = 2$ и $(p-1)^2 \equiv 1 \pmod{q}$. Значит, либо $p-1 \equiv 1 \pmod{q}$, либо $p-1 \equiv -1 \pmod{q}$.

В первом случае получаем, что $(p-1)^n \equiv 1^n = 1 \equiv -1 \pmod{q}$ — противоречие. Значит, $p-1 \equiv -1 \pmod{q}$ и $p = q$.

Далее, из условия $n \leqslant 2p$ получаем, что $n = p$ (т.к. n нечетно). Значит, $(p-1)^p + 1 \vdots p^{p-1}$.

Применим LTE-2:

$$\|(p-1)^p + 1\|_p = \|(p-1) + 1\|_p + \|p\|_p = 2.$$

С другой стороны, $\|(p-1)^p + 1\|_p \geqslant p-1$. Значит, $2 \geqslant p-1$ и $p \leqslant 3$. Окончательно получаем, что $p = n = 3$.

Ответ: $n = 1$, p — любое простое; $n = p = 2$; $n = p = 3$.

86. Для каждого натурального k обозначим через $C(k)$ сумму всех простых различных делителей числа k. Например $C(1) = 0$, $C(2) = 2$, $C(45) = 8$. Найдите все натуральные n для которых $C(2^n + 1) = C(n)$.

Решение. Прежде всего заметим, что если $p > 3$ — простое, то у числа $2^p + 1$ все простые делители больше p. В самом деле, пусть $2^p \equiv -1 \pmod{q}$, где q простое. Тогда $2^{2p} \equiv 1 \pmod{q}$, поэтому показатель 2 по модулю q равен 2 или $2p$. В первом случае получаем, что $q = 3$, а во втором — что $q > 2p > p$. Теперь рассмотрим два случая.

Пусть n нечетно и $p_1 < \ldots < p_k$ — все его простые делители, упорядоченные по возрастанию. Тогда по теореме Зигмонди у каждого из чисел $2^{p_i}+1$ есть простой делитель q_i, который отличен от $2^1 + 1 = 3$ и которого нет у чисел $2^{p_j} + 1$ при $p_j < p_i$. Значит, каждое число $2^{p_i} + 1$ порождает простой делитель $q_i > p_i$, если только $p_i \neq 3$. Осталось заметить, что $2^{p_i} + 1 \mid 2^n + 1$, поэтому если $n \neq 3$, то $C(2^n + 1) > C(n)$. Так что $n = 3$ — единственный ответ при нечетном n.

Теперь пусть n четно. Ясно, что у числа n должен быть хотя бы один нечетный простой делитель. Обозначим через $2 < p_2 < \ldots < p_k$ все его простые делители. Далее, положим $a = 2^{2^\alpha}$ и применим теорему Зигмонди к числам $a^{p_i} + 1$. Тогда у числа $a^{p_i} + 1$ есть простой делитель q_i, которого нет у всех $a^{p_j} + 1$ при $p_j < p_i$, а также этого делителя нет у числа $a + 1$. Докажем, что $q_i > p_i + 2$. В самом деле, $a^{2p_i} \equiv 1 \pmod{q_i}$. Показатель числа a по модулю q не может быть равен 1 (т.к. тогда $q_i = 2$, что невозможно), 2 (т.к. в противном случае $a \equiv -1 \pmod{q_i}$ и $q_i \mid a + 1$, что также невозможно) и p_i. Значит, он равен $2p_i$ и $q_i > 2p_i > p_i + 2$. Поскольку $a^{p_i+1} \mid 2^n + 1$, то у числа $2^n + 1$ есть $(k-1)$ простой делитель $q_2, \ldots, q_k$, причем их сумма больше суммы $p_2 + \ldots + p_k + 2$. Значит, $C(2^n + 1) > C(n)$, и в случае четного n решений нет.

Ответ: $n = 3$.

87. Пусть n — произвольное натуральное число. Докажите, что у числа $2^{2^n} + 2^{2^{n-1}} + 1$ есть не менее 2^n натуральных делителей.

Решение. Достаточно доказать, что у числа $2^{2^n} + 2^{2^{n-1}} + 1$ есть хотя бы n простых делителей (не обязательно различных). Заметим, что

$$2^{2^n} + 2^{2^{n-1}} + 1 = \Phi_3(2^{2^{n-1}}) = \Phi_{3 \cdot 2^{n-1}}(2) = \prod_{d \mid 2^{n-1}} \Phi_{3d}(2),$$

причем $|\Phi_{3d}(2)| > 1$ при всех натуральных d. Таким образом, мы представили число $2^{2^n}+2^{2^{n-1}}+1$ в виде произведения n целых множителей, больших 1 по модулю. Взяв в каждом множителе простой делитель, которого нет у предыдущих множителей (это возможно по теореме Зигмонди), получаем требуемое.

88. Найдите все натуральные k такие, что произведение первых k простых чисел, уменьшенное на 1, является точной степенью натурального числа (большей, чем первая).

Решение. Пусть $p_1 \dots p_k = a^n + 1$. При $a = 1$ получаем $k = 1$. Пусть теперь $a > 1$ и $k > 1$. Тогда $a > p_k$, поскольку в противном случае найдется $p_i \mid a$ и правая часть не может быть кратна p_i. Пусть теперь $q \mid n$ — некоторый простой делитель. Тогда $q > 2$, т.к. $a^2 + 1$ не может делиться на $p_2 = 3$. Докажем, что $q > p_k$. В самом деле, в противном случае по малой теореме Ферма $0 \equiv (a^{n/q})^q + 1 \equiv a^{n/q} + 1 \pmod q$ и по LTE-2 имеем

$$1 = \|p_1 \dots q \dots p_k\|_q = \|a^n + 1\|_q = \|a^{n/q} + 1\|_q + \|q\|_q \geqslant 2,$$

что невозможно. Значит, $q > p_k$ и $n > p_k$, откуда

$$a^n + 1 > p_k^{p_k} > p_1 \dots p_k$$

— противоречие.

Ответ: $k = 1$.

89. Дано натуральное $k > 1$. Докажите, что существует бесконечно много натуральных n таких, что $n \mid 1^n + 2^n + 3^n + \ldots + k^n$.

Решение. В случае четного k положим $n = (k+1)^a$. Тогда если $p \mid n$ — произвольный простой делитель, то по LTE-2 имеем

$$\|a^n + (k+1-a)^n\|_p = \|a + (k+1-a)\|_p + \|n\|_p \geqslant \|n\|_p + 1,$$

так что делимость выполнена.

В случае нечетного k положим $n = k^a$. Тогда если $p \mid n$ — произвольный простой делитель, то по LTE-2 имеем

$$\|a^n + (k-a)^n\|_p = \|a + (k-a)\|_p + \|n\|_p \geqslant \|n\|_p + 1,$$

так что делимость также выполнена.

90. Докажите, что последовательность $a_n = 3^n - 2^n$ не содержит трех последовательных членов геометрической прогрессии.

Решение. Достаточно применить теорему Зигмонди к числу $3^{n+1} - 2^{n+1}$ и заметить, что у него есть простой делитель, которого нет у числа $3^n - 2^n$, а значит, равенство

$$(3^n - 2^n)^2 = (3^{n-1} - 2^{n-1})(3^{n+1} - 2^{n+1})$$

невозможно.

91. Докажите, что уравнение $x^n + y^n = p^n$ не имеет натуральных решений при $n \geqslant 3$ и простом p.

Решение. Если n имеет нечетный простой делитель q, то достаточно доказать, что у уравнения $a^q + b^q = p^n$ нет натуральных решений. Для этого заметим, что $p \mid a + b$ и применим теорему Зигмонди к числу $a^q + b^q$. получаем, что у этого числа должен быть простой делитель, отличный от p, что невозможно.

Если же $n = 2^k$ и $k \geqslant 2$, то, во-первых, x и y взаимно просты, а во-вторых, одно из чисел x или y должно быть четным. Пусть $y = 2z$; положим $x^{2^{k-2}} = a$ и $2^{2^{k-1}} z^{2^{k-2}} = b$. Тогда

$$p^{2^k} = a^4 + 4b^4 = (a^2 - 2ab + 2b^2)(a^2 + 2ab + 2b^2).$$

Значит, обе скобки — это степени p. Но тогда их разность, равная $4ab$, кратна p. Т.к. $p \nmid ab$, получаем, что $p = 2$. Но тогда $x^n + y^n > 2^n$ — противоречие.

92. Докажите, что для любого простого p многочлен $x^4 + 1$ приводим над полем $\mathbb{Z}_p$.

Решение. Способ 1. Если $p = 1$, то возьмем $n = 1$. Если $p \equiv 1 \pmod 8$, то рассмотрим первообразный корень g по модулю p и положим $n = g^{(p-1)/8}$. Тогда $x - n \mid x^4 + 1$. Если же $p \not\equiv 1 \pmod 8$, то, как известно, $8 \mid p^2 - 1$, поэтому в поле $\mathbb{F}_{p^2}$ если элемент порядка 8 согласно задаче 54. С другой стороны, такого элемента нет в поле $\mathbb{Z}_p$. Значит, минимальный многочлен этого элемента квадратичен и потому является нетривиальным делителем многочлена $\Phi_8(x) = x^4 + 1$.

Способ 2. Рассмотрим четыре корня уравнения $x^4 + 1 = 0$:

$$z_1 = \frac{1+i}{\sqrt{2}}, \quad z_2 = \frac{-11+i}{\sqrt{2}}, \quad z_3 = \frac{-1-i}{\sqrt{2}}, \quad z_4 = \frac{1-i}{\sqrt{2}}.$$

Заметим, что

$$x^4 + 1 = (x - z_1)(x - z_2)(x - z_3)(x - z_4).$$

Будем группировать скобки в правой части равенства на пары тремя способами:

$$\Big((x - z_1)(x - z_2)\Big)\Big((x - z_3)(x - z_4)\Big) = (x^2 - \sqrt{-2}x - 1)(x^2 + \sqrt{-2}x - 1),$$
$$\Big((x - z_1)(x - z_4)\Big)\Big((x - z_2)(x - z_3)\Big) = (x^2 - \sqrt{2}x + 1)(x^2 + \sqrt{2}x + 1),$$
$$\Big((x - z_1)(x - z_3)\Big)\Big((x - z_2)(x - z_4)\Big) = (x^2 - \sqrt{-1})(x^2 + \sqrt{-1}).$$

Заметим, что одно из чисел $\sqrt{-1}$, $\sqrt{2}$ и $\sqrt{-2}$ обязательно будет квадратичным вычетом по модулю p. Соответствующее разложение в таком случае и будет искомым.

93. Пусть $\{a_n\}$ — монотонно возрастающая последовательность натуральных чисел. Докажите, что множество простых делителей чисел вида $a_i + a_j$ (где $i \neq j$) бесконечно.

Решение. Предположим противное: пусть существует лишь конечное число простых делителей и чисел вида $a_i + a_j$. Обозначим эти делители через $p_1, \ldots, p_k$. Зафиксируем числа $a_1, a_2, \ldots, a_{k+1}$ и будем рассматривать суммы $a_1 + a_t, a_2 + a_t, \ldots, a_{k+1} + a_t$. Заметим, что

$$(a_i + a_t, a_j + a_t) = (a_i + a_t, a_i - a_j) \leqslant |a_i - a_j| \quad \text{при всех } t.$$

С другой стороны, максимальная примарная компонента числа вида $a_i + a_t$ не меньше $\sqrt[k]{a_i + a_t}$ и неограниченно растет при $t \to \infty$. Но тогда при каждом t у двух чисел $a_i + a_t$ и $a_j + a_t$ простой делитель максимальной примарной компоненты общий, а потому их НОД делится на меньшую такую примарную компоненту. Значит, такой НОД неограниченно возрастает — противоречие.