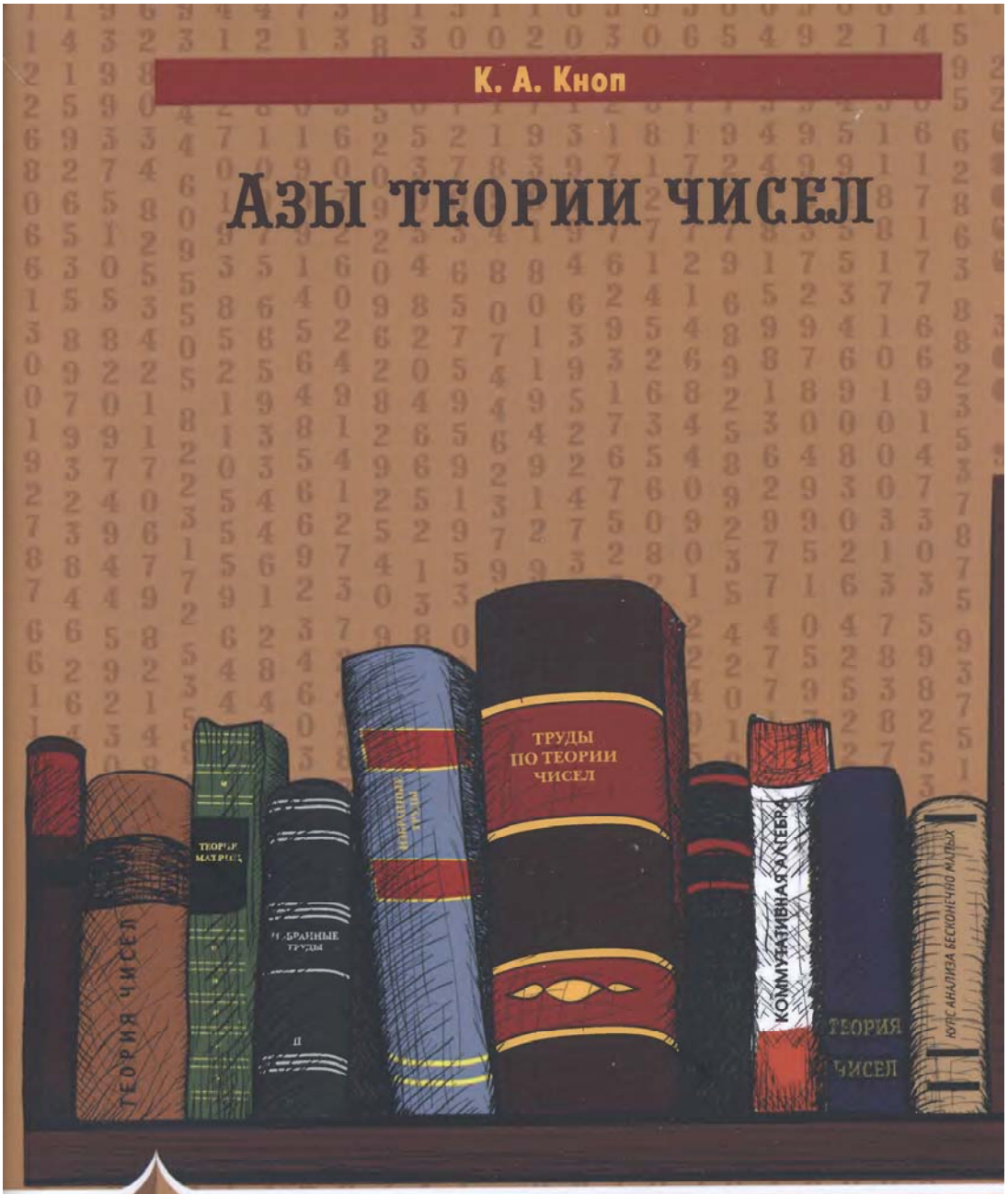
К. А. Кноп

Азы теории чисел



Школьные
Математические
Кружки

К. А. Кноп

Азы теории чисел

Издательство МЦНМО
Москва, 2017

УДК 511
ББК 22.1
К53

Кноп К. А.

К53 Азы теории чисел. — М.: МЦНМО, 2017. — 80 с.

ISBN 978-5-4439-1126-7

Шестнадцатая книжка серии «Школьные математические кружки» посвящена арифметике остатков. В неё вошли разработки семи занятий математического кружка для 7—9 классов с подробно разобранными примерами различной сложности, задачами для самостоятельного решения и методическими указаниями для учителя. В конце книги приведены дополнительные задачи и их решения.

Книга продолжает брошюру А. И. Сгибнева «Делимость и простые числа», переходя от вопросов делимости к математическим понятиям и языку, чьё появление произвело революцию в теории чисел. Рассматриваются теорема Вильсона, свойства функции Эйлера, китайская теорема об остатках, малая теорема Ферма и теорема Эйлера. Последние два занятия посвящены новым для кружков темам: псевдопростым числам и криптографии с открытым ключом.

Для удобства использования заключительная часть книжки, как всегда, сделана в виде раздаточных материалов. Книжка адресована школьным учителям математики и руководителям математических кружков. Надеемся, что она будет интересна школьникам и их родителям, студентам педагогических вузов, а также всем любителям математики.

12+

ISBN 978-5-4439-1126-7

Предисловие

Восьмым выпуском в серии «Школьные математические кружки» вышла книга А. И. Сгибнева «Делимость и простые числа» (в дальнейшем мы будем обозначать ее ДПЧ). В ней несколько первых занятий посвящены вопросам делимости натуральных чисел, рассказывается о свойствах деления (в том числе доказывается теорема об однозначности деления с остатком), а также о признаках делимости, но ничего не сказано об *арифметике остатков* (*модулярной арифметике*), то есть о том математическом языке, появление которого в своё время произвело настоящую революцию в теории чисел — разделе математики, изучающем целые числа. Настоящая книжка является логическим продолжением ДПЧ, поэтому мы начинаем её с рассказа об этом языке. На следующих занятиях рассматриваются теорема Вильсона, свойства функции Эйлера, китайская теорема об остатках, малая теорема Ферма и теорема Эйлера. Все эти темы почти независимы друг от друга и могут изучаться в любом порядке (хотя некоторые решения задач опираются на теоремы из предыдущих занятий).

Последние два занятия посвящены темам, которые для теории чисел являются относительно новыми (а для кружковых занятий — совсем новыми) — псевдопростым числам и криптографии с открытым ключом.

Все семь занятий предназначены для учеников 7—9 классов, хотя могут быть использованы и в кружках 10—11 классов.

В то же время ряд более классических числовых тем — квадратичные вычеты и невычеты, закон взаимности, решение разнообразных диофантовых уравнений высоких степеней — в эту книгу уже явно не помещались[1].

[1]Автор надеется впоследствии вернуться к ним в следующей книжке — «Буки теории чисел». Так как буква А славянской азбуки раньше называлась «Аз», а буква Б — «Буки», продолжением «азов теории чисел» должны являться именно «буки», не так ли?

Подавляющее большинство задач не новы. Многие из них встречалась в различных англоязычных учебниках по началам теории чисел. Автор выражает признательность А. С. Штерну и особенно А. В. Шаповалову, предложившим ряд ценных улучшений текста книги.

Говоря о числах и их делителях, мы подразумеваем целые числа и натуральные делители. Буквами p и q, как правило, обозначены простые числа.

Большая часть обозначений общеприняты и стандартны. Среди не самых стандартных обозначений упомянем три:

$n!!$ — произведение всех натуральных чисел, не превосходящих натурального числа n и имеющих с ним одинаковую чётность (например, $5!! = 1 \cdot 3 \cdot 5 = 15$);

$m \perp n$ — обозначение для взаимной простоты чисел:

$$m \perp n \Leftrightarrow \text{НОД}(m, n) = 1;$$

этот же значок для простого n является краткой формой записи слов «m не делится на n»;

скобки Айверсона[1]:

$$[\text{утверждение}] = \begin{cases} 1, & \text{если утверждение истинно,} \\ 0, & \text{если утверждение ложно.} \end{cases}$$

С помощью скобок Айверсона легко выражать многие нестандартные математические функции через стандартные. Например, $\max(x, y) = x[x > y] + y[x \leqslant y]$, $\delta_{ij} = [i = j]$ (символ Кронекера), $\operatorname{sgn}(x) = [x > 0] - [x < 0]$. Скобки Айверсона внутри сумм используются для суммирования только по тем индексам, для которых утверждение истинно. Например,

$$\sum_{P(k)} a_k = \sum a_k[P(k)],$$

а

$$\sum_{1 \leqslant d \leqslant n} [d \perp n] = \sum [d \perp n][1 \leqslant d \leqslant n] = \varphi(n).$$

Для целой части числа x мы используем обозначение $\lfloor x \rfloor$.

[1]Обозначение предложено в 1960 году Кеннетом Юджином Айверсоном (1920—2004) — канадским учёным и программистом, автором языка программирования APL.

Кроме того, в книге содержится много ссылок на числовые последовательности из онлайн-энциклопедии целочисленных последовательностей http://oeis.org. В качестве ссылок мы используем номера последовательностей в онлайн-энциклопедии. Например, A000027 означает ссылку http://oeis.org/A000027.

Занятие 1

Арифметика остатков

Если $m > 1$ и $(a - b) \vdots m$, то говорят, что a и b *сравнимы по модулю* m. Сравнимость записывают так: $a \equiv b \pmod{m}$. Если значение модуля очевидно из контекста, то скобки с указанием модуля обычно опускают.

Использование записи $a \equiv b$ вместо $(a - b) \vdots m$ оказывается очень удобным и мощным инструментом в разных задачах, потому что со сравнениями, как мы сейчас убедимся, можно действовать как с равенствами: складывать, вычитать, умножать, иногда делить.

Задача 1.1. Докажите, что если $a \equiv b \pmod{m}$ и $c \equiv d \pmod{m}$, то

а) $a + c \equiv b + d \pmod{m}$;

б) $ac \equiv bd \pmod{m}$.

Решение. а) $(a + c) - (b + d) = (a - b) + (c - d)$. Так как каждая скобка в правой части равенства делится на m, их сумма (разность скобок в левой части равенства) также кратна m. Это и означает, что $a + c \equiv b + d$.

б) $ac - bd = a(c - d) + d(a - b)$. Из условия следует, что $a - b \vdots m$ и $c - d \vdots m$, поэтому $ac - bd \vdots m$.

Задача 1.2. Докажите, что если $a \equiv b \pmod{m}$ и k — натуральное число, то $a^k \equiv b^k \pmod{m}$.

Указание. Один способ доказательства — с помощью алгебраического тождества

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

Другой способ — с помощью математической индукции, многократно применяя умножение сравнений (задачу 1.1б).

Мы будем говорить, что множество M образует *полную систему остатков* по модулю m, если для каждого целого числа существует ровно один сравнимый с ним (по модулю m) элемент этого множества. Чаще всего в

Карл Фридрих Гаусс (1777—1855) — немецкий математик, астроном и физик. Ещё в детстве проявил яркие способности к математике и иностранным языкам. В возрасте 19 лет построил с помощью циркуля и линейки правильный 17-угольник — это стало первым продвижением в задаче о построении правильных многоугольников со времён Евклида. В 24 года опубликовал знаменитые «Арифметические исследования», в которых, в частности, изложил теорию квадратичных вычетов и сравнений второй степени, включающую «квадратичный закон взаимности». Именно в этой книге впервые был применён современный язык сравнений, сделавший возможным работу с делимостью чисел как с равенствами.

В зрелом возрасте Гаусс активно занимался алгеброй, астрономией, геодезией, был избран иностранным членом многих академий наук, включая и Петербургскую. Его научные интересы были столь разносторонними, а вклад в математические науки столь весомым, что его назвали «королём математиков».

качестве полной системы остатков выбирается множество $\{0, 1, 2, \ldots, m-1\}$ или множество $\{1, 2, \ldots, m\}$.

Комментарий. В этом определении можно заменить условие единственности сравнимого элемента на условие $|\mathrm{M}| = m$ или даже на $|\mathrm{M}| \leqslant m$. Действительно, если для каждого целого числа есть хотя бы один сравнимый с ним элемент

множества и при этом общее количество элементов M не больше m, то двух различных элементов, сравнимых с одним и тем же числом, быть не может.

Задача 1.3. Пусть m — натуральное число. Докажите, что множество $\mathrm{M} = \{0, 3, 6, \ldots, 3m - 3\}$ образует полную систему остатков тогда и только тогда, когда $m \perp 3$.

Решение. Сначала докажем простую (почти очевидную) часть этого утверждения. Если $m \vdots 3$, то $m \in \mathrm{M}$, потому что $m < 3m - 3$, а M содержит все числа, кратные 3 и не превосходящие $3m - 3$. Но так как $m \equiv 0 \pmod{m}$, M содержит хотя бы два различных элемента, сравнимых с числом m (а именно, 0 и m). Следовательно, M не образует полной системы остатков.

Если же $m \perp 3$, то $m = 3k + 1$ или $m = 3k + 2$ для некоторого натурального k. Разберем первый случай (второй рассматривается аналогично):

$$\mathrm{M} = \{0, 3, 6, \ldots, 3k, 3k + 3, \ldots, 6k, 6k + 3, \ldots, 9k\}.$$

Все числа от 0 до $3k$ оставим на месте, а вместо чисел от $3k + 3$ до $6k$ выпишем числа, меньшие их на m (это сохраняет единственность сравнимого элемента множества): получатся числа $2, 5, \ldots, 3k - 1$. Точно так же для чисел от $6k + 3$ до $9k$ выпишем вместо них числа, меньшие их на $2m = 6k + 2$ — получатся числа $1, 4, \ldots, 3k - 2$. В итоге получились все числа от 0 до $3k$ (то есть до $m - 1$), каждое число встречается ровно один раз. Следовательно, система остатков является полной.

Задача 1.4. Постройте таблицу умножения по модулю 5.

Решение.

mod 5	**1**	**2**	**3**	**4**
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Задача 1.5. Постройте таблицу умножения по модулю 6.

Решение.

mod 6	1	2	3	4	5
1	1	2	3	4	5
2	2	4	0	2	4
3	3	0	3	0	3
4	4	2	0	4	2
5	5	4	3	2	1

Вопросы по таблицам:

1) Почему в первой таблице не было нулей, а во второй они есть?

2) Почему в каждой строчке первой таблицы никакое число не повторяется дважды?

3) Для каких модулей в пределах первого десятка таблицы умножения будут похожи на таблицу по модулю 5, а для каких — на таблицу по модулю 6?

4) Сколько в таблице по модулю 12 таких строчек, в которых нет нулей?

Ответы на эти вопросы:

1) Потому что 5 — простое число, а 6 — составное. Когда перемножаются два числа, одно из которых кратно 2, а другое кратно 3, то в результате (в таблице по модулю 6) получается 0.

2) Ровно по той же причине: если бы $ab \equiv ac$ при разных b и c, то в той же строчке должен был быть 0: $a(b-c) \equiv 0$. Но по простому модулю это невозможно.

3) По-видимому, для простых модулей (то есть чисел 2, 3, 7) таблицы будут аналогичны таблице по модулю 5 (нет нулей, все числа в каждом столбце и каждой строке различны), а для составных — аналогичны таблице по модулю 6.

4) Этот вопрос сформулируем по-другому: для каких множителей $m < 12$ не может выполняться равенство $mn \equiv 0$ ни при каких $n < 12$? Невозможность такого равенства равносильна условию $m \perp 12$. Иначе говоря, $m = 1, 5, 7$ или 11. Ответ: 4 строчки.

Задачи для самостоятельного решения

Задача 1.6. Найдите наименьшие неотрицательные остатки для $6^k + 1 \pmod{17}$ при $k = 1, 2, 3, 4, 5$.

Задача 1.7. а) Пусть m — нечётное натуральное число. Докажите, что множество $\{0, 2, 4, \ldots, 2m - 2\}$ — полная система остатков по модулю m. б) Пусть $k \perp m$. Докажите, что множество $\{0, k, 2k, \ldots, (m-1)k\}$ — полная система остатков по модулю m. в) Пусть $k \perp m$, r — произвольное число. Докажите, что $\{r, k + r, 2k + r, \ldots, (m-1)k + r\}$ — полная система остатков по модулю m.

Задача 1.8. Пусть $d \perp m$ и $ad \equiv bd \pmod{m}$. Тогда $a \equiv b \pmod{m}$.

Задача 1.9. Пусть d — натуральное число, являющееся общим делителем a, b и m. Докажите, что сравнения $a \equiv b \pmod{m}$ и $a/d \equiv b/d \pmod{m/d}$ равносильны.

Задача 1.10. Пусть $p(x)$ — многочлен с целыми коэффициентами и $a \equiv b \pmod{m}$. Тогда $p(a) \equiv p(b) \pmod{m}$.

Задача 1.11. Докажите, что $7^{2014} + 9^{2014} \vdots 10$.

Задача 1.12. Докажите, что ни при каком натуральном n число $3^n + 5^n$ не является полным квадратом.

Задача 1.13. Последовательность (a_n) задана формулами $a_1 = a_2 = 1$, $a_{n+2} = a_n a_{n+1} + 1$. Докажите, что $a_n - 3$ — составное число при $n > 6$.

См. также задачи Д1—Д18.

Решения и указания

1.6. $6^1 + 1 = 7$, $6^2 + 1 \equiv 2 + 1 = 3 \pmod{17}$. Дальше проще считать сразу «в остатках», учитывая предыдущие найденные остатки для степеней шестёрки, перемножая нужные из них и затем добавляя к результату единицу:

$$6^3 + 1 \equiv 6 \cdot 2 + 1 = 13,$$

$$6^4 + 1 \equiv 2 \cdot 2 + 1 = 4 + 1 = 5,$$

$$6^5 + 1 \equiv 6 \cdot 4 + 1 \equiv 7 + 1 = 8.$$

1.7. Указание. Решение всех пунктов аналогично второй части решения задачи 1.3.

1.8. По условию $d(a-b) \vdots m$ и $d \perp m$. Следовательно, $(a-b) \vdots m$, а это и означает, что $a \equiv b \pmod{m}$.

1.9. Пусть $a = da'$, $b = db'$, $m = dm'$. Тогда первое сравнение эквивалентно условию $(a-b) \vdots m$, то есть $(da' - db') \vdots dm'$, а второе сравнение эквивалентно условию $(a' - b') \vdots m'$. Очевидно, что два последних утверждения равносильны.

1.10. Указание. Запишите многочлен в стандартном виде, после чего воспользуйтесь результатами задач 1.1 и 1.2 и методом математической индукции.

1.11. Найдем несколько первых степеней семёрки по модулю 10: $7^1 = 7$, $7^2 = 49 \equiv 9$, $7^3 = 7 \cdot 49 \equiv 7 \cdot 9 \equiv 3$, $7^4 \equiv 7 \cdot 3 \equiv 1$. Так как $2014 = 4 \cdot 503 + 2$, получаем $7^{2014} = (7^4)^{503} \cdot 7^2 \equiv \equiv 1^{503} \cdot 9 \equiv 9 \pmod{10}$. Аналогично для степеней девятки: $9^2 = 81 \equiv 1$, и поэтому $9^{2014} = (9^2)^{1007} \equiv 1^{1007} = 1$. Следовательно, $7^{2014} + 9^{2014} \equiv 9 + 1 \equiv 0 \pmod{10}$.

Комментарий. Совсем нетрудно убедиться, что степени натуральных чисел всегда «зацикливаются» (по любому модулю). Это следует из того, что количество различных остатков конечно, а так как количество натуральных степеней бесконечно, какой-то остаток обязательно встретится второй раз. Далее из свойства произведения сравнений следует, что все последующие остатки тоже будут повторены, т. е. возникнет цикл остатков. В решении задачи мы фактически нашли такой цикл (и для семёрки, и для девятки) и воспользовались тем, что в нём есть остаток 1.

1.12. Поначалу совершенно непонятно, какое отношение эта задача имеет к сравнениям по модулю. Поэтому начнём с того, что просто сосчитаем несколько первых чисел вида $3^n + 5^n$:

$$3^1 + 5^1 = 8, \quad 3^2 + 5^2 = 34 = 2 \cdot 17, \quad 3^3 + 5^3 = 152 = 8 \cdot 19,$$
$$3^4 + 5^4 = 706 = 2 \cdot 353, \quad 3^5 + 5^5 = 3368 = 8 \cdot 421.$$

Возникает гипотеза: $3^n + 5^n$ при нечётных показателях степени делится на 8, но не делится на 16, а при чётных — делится на 2, но не делится на 4. А так как двойка в разложение полного квадрата входит всегда в чётной степени, выражение $3^n + 5^n$ полным квадратом быть не может. Осталось это доказать с помощью сравнений по модулю. Теперь

уже понятно, что выбирать нужно модуль 16, чтобы получить по нему 8 для нечётных степеней и какие-то ещё не кратные 4 числа для чётных. Цикл для степеней 3 по модулю 16: 1, 3, 9, 11, 1. Цикл для степеней 5: 1, 5, 9, 13, 1. Оба цикла имеют длину 4, поэтому $3^n + 5^n$ тоже даёт цикл длины не более 4: $1 + 1 = 2$, $3 + 5 = 8$, $9 + 9 \equiv 2$, $11 + 13 \equiv 8$, $1 + 1 = 2$. Выясняется, что длина этого цикла на самом деле равна 2, и он состоит только из двоек и восьмёрок, откуда и получается утверждение задачи.

1.13. Эта задача кажется ещё более далёкой от темы, чем предыдущая. Тем не менее, выпишем несколько первых значений и попробуем разобраться: $a_1 = 1$, $a_2 = 1$, $a_3 = 2$, $a_4 = 3$, $a_5 = 7$, $a_6 = 22$, $a_7 = 155$, $a_8 = 3411$, $a_9 = 528706$. (A007660)

Для a_7 и a_8 очевидно, что результат после вычитания 3 не будет простым числом: в результате получались чётные числа. Однако то, что $a_9 - 3 = 528703$ не является простым, как минимум не очевидно. А дальше члены последовательности начинают расти так, что даже вычисление десятого члена без калькулятора уже затруднительно. Изюминка этой задачи состоит в том, что такие громоздкие вычисления вовсе не нужны! Достаточно того, что мы легко можем считать члены этой последовательности по модулю, равному одному из предыдущих членов: $a_{n+1} \equiv 1 \pmod{a_n}$, $a_{n+2} \equiv 1 \pmod{a_n}$, поэтому $a_{n+3} \equiv 1 \cdot 1 + 1 = 2 \pmod{a_n}$, $a_{n+4} \equiv 2 \cdot 1 + 1 = 3 \pmod{a_n}$, $a_{n+5} \equiv 3 \cdot 2 + 1 = 7 \pmod{a_n}$. Этого уже хватает, даже с запасом: так как $a_{n+4} \equiv 3 \pmod{a_n}$, получаем, что $(a_{n+4} - 3) \vdots a_n$, причем $a_n > 1$ при $n > 2$. А значит, $a_{n+4} - 3$ является составным числом.

Занятие 2

Решение сравнений. Теорема Вильсона

Это занятие почти целиком посвящено решению простейших сравнений, то есть нахождению остатков, которые удовлетворяют данному сравнению. Как правило, мы не будем выходить за рамки сравнений первой степени с одной переменной, то есть таких, в которых левая и правая части сравнения являются линейными многочленами.

Каждое сравнение $ax - c \equiv 0 \pmod{b}$, как легко видеть, эквивалентно уравнению $ax + by = c$, которое необходимо решить в целых числах. Решениями x такого сравнения мы будем считать все различные остатки (по модулю b), которые удовлетворяют этому сравнению. Но прежде чем его решать, мы постараемся сократить числа a, b, c на их общий делитель[1].

Случай 1. Если $\text{НОД}(c, b) = d > 1$ и a делится на d, то сравнение $ax \equiv c \pmod{b}$ равносильно сравнению $a'x \equiv c' \pmod{b'}$, где $(a', b', c') = (a/d, b/d, c/d)$.

Задача 2.1. Пусть $d = \text{НОД}(c, b)$. Докажите, что любое решение сравнения $x \equiv c \pmod{b}$ делится на d, то есть $x \equiv 0 \pmod{d}$. При этом x/d является решением сравнения $x/d \equiv c/d \pmod{b/d}$.

Решение. Условие $d = \text{НОД}(b, c)$ означает, что $c = dc'$ и $b = db'$, причём $c' \perp b'$. Так как $x - c = by$, имеем $x = c + by = d(c' + b'y)$, что равносильно $x \equiv 0 \pmod{d}$ и $x/d = c' \pmod{b'}$.

Что будет после сокращения на d, то есть когда уже $\text{НОД}(c, b) = 1$? Может оказаться, что $\text{НОД}(a, b) = d > 1$. Этот случай самый простой: левая часть уравнения

$$ax + by = c$$

[1] Точно так же мы поступали в школе с любыми другими уравнениями. Например, вместо уравнения $14x = 77$ всегда решают уравнение $2x = 11$, полученное в результате сокращения на 7.

делится на d, а правая нет, поэтому уравнение не может иметь целых решений. Таким образом, имеет место

Случай 2. Сравнение $ax \equiv c \pmod{b}$ неразрешимо, если НОД$(a, b) > 1$, а НОД$(c, b) = 1$.

Теперь разберемся со *случаем* 3, в котором НОД$(a, b) = 1$, но НОД$(a, c) = d > 1$. Что делать в такой ситуации, мы продемонстрируем в двух следующих задачах.

Задача 2.2. Пусть b — нечетное число и $2ax \equiv 2c \pmod{b}$. Докажите, что $ax \equiv c \pmod{b}$.

Решение. Условие означает, что $2ax - 2c \vdots b$, то есть $2(ax - c) = bq$, где q — целое число. Левая часть выражения чётна, значит, и правая часть чётна. Но так как b нечётно, чётным должно быть q. Запишем $q = 2q'$, $2(ax - c) = 2bq'$. Отсюда $ax - c = bq'$, то есть $ax - c \equiv 0 \pmod{b}$.

Задача 2.3. Пусть $b \perp k$ (т. е. НОД$(k, b) = 1$). Докажите, что сравнение $axk \equiv ck \pmod{b}$ можно сократить на k: из $axk \equiv ck \pmod{b}$ следует, что $ax \equiv c \pmod{b}$.

Решение. Доказательство утверждения этой задачи полностью аналогично предыдущему.

Задача 2.4. Докажите, что если $d =$ НОД$(a, b) > 1$, то сравнение $ax \equiv 0 \pmod{b}$ имеет ненулевое решение.

Решение. По условию $b = db'$ и $a = da'$, причём $0 < b' < b$. Тогда $ab' = a'b$ делится на b, так что b' — искомое решение.

Комментарий. Из задач 2.2—2.4 вытекает следующее утверждение: обе части сравнения $ak \equiv ck \pmod{b}$ можно сокращать на k тогда и только тогда, когда $b \perp k$.

Задача 2.5. Докажите, что если p — простое число, то:

а) в каждой строке таблицы умножения остатков по модулю p встречается ровно одна единица;

б) единица может стоять на диагонали только в первой и последней строках;

в) числа, сравнимые с $2, 3, 4, \ldots, (p - 3), (p - 2)$ можно разбить на пары так, что произведение чисел в каждой паре будет сравнимо с единицей по модулю p;

г) $(p - 1)! \equiv -1 \pmod{p}$.

Решение. а) Это частный случай утверждения о том, что в каждой строке записана полная система остатков — см. задачу 1.7б.

Джон Вильсон (Уилсон) (1741—1793) — английский математик и юрист. Теорема, носящая ныне его имя, впервые была сформулирована без доказательства его учителем Эдвардом Варингом (Уорингом) в 1770 году в труде «Meditationes Algebraicae». Первое доказательство теоремы Вильсона дал в 1771 году Жозеф Луи Лагранж.

б) На диагонали стоят числа $a \cdot a$. Если $a^2 \equiv 1 \pmod{p}$, то $(a-1)(a+1) \equiv 0 \pmod{p}$, откуда $a - 1 \equiv 0$ или $a + 1 \equiv 0$. Первое сравнение соответствует первой строке ($a = 1$), второе — последней ($a = p - 1$).

в) Из пункта а) следует, что в каждой строке $2, 3, \ldots, p-2$ встречается ровно одна единица, а из пункта б) следует, что она не находится на диагонали, то есть номер её столбца не совпадает с номером строки. Если в i-й строке единица стоит в j-м столбце, то в j-й строке единица будет в i-м столбце (в силу симметричности таблицы умножения). А это и означает, что соответствие, при котором числу i ставится в соответствие число j, задаёт разбиение всех чисел на пары.

г) Вместо перемножения всех чисел от 1 до $p - 1$ подряд мы перемножим все найденные в п. в) пары чисел друг на

друга (каждый результат при этом равен 1). Тогда произведение сравнимо с $1 \cdot 1 \cdot \ldots \cdot 1 \cdot (-1) = -1$.

Задача 2.6 (теорема Вильсона). Докажите, что

$$(p-1)! + 1 \vdots p \Leftrightarrow (p \text{ — простое число}).$$

Решение. В задаче 2.5г доказана достаточность условия «p — простое». Осталось доказать его необходимость. Предположим противное: p — составное. Тогда среди чисел, меньших p, есть делители p. Если n и p/n — два таких делителя, то они оба входят множителями в $(p-1)!$, а значит, $(p-1)! \vdots p$. Поэтому $(p-1)! + 1 \perp p$.

Мы разобрали все случаи сократимости коэффициентов сравнения. Теперь самое время разобраться с несократимым случаем.

Остаток $a \pmod b$ назовём *обратимым*, если существует *обратный* к нему остаток, то есть такой a', для которого $aa' \equiv 1 \pmod b$. Для a' мы будем использовать обозначение $1/a$.

Задача 2.7. а) Докажите, что если $a \perp b$, то остаток a обратим.

б) Докажите, что если остаток $a \pmod b$ обратим, то $a \perp b$.

в) Докажите, что если $a \perp b$, то решением сравнения $ax \equiv c \pmod b$ является $c/a \pmod b$, то есть $c \cdot (1/a)$.

Решение. а) Если $a \perp b$, то (по основной лемме из занятия 6 книги ДПЧ) существуют такие целые числа x и y, что $ax + by = 1$. Это значит, что $ax \equiv 1 \pmod b$, то есть $x = 1/a$.

б) Если $aa' \equiv 1 \pmod b$, то существует целое k, для которого $aa' - 1 = kb$, $aa' - kb = 1$. Любой общий делитель чисел a и b делит и выражение $aa' - kb$, а значит, НОД$(a, b) = 1$, то есть $a \perp b$.

в) Домножим обе части сравнения на $1/a$. Получим равносильное сравнение (кстати, почему оно равносильно, а не является неравносильным следствием?):

$$(1/a)ax \equiv (1/a)c \pmod b,$$

то есть $x \equiv c/a \pmod b$.

Задачи для самостоятельного решения

Задача 2.8. Найдите все решения сравнений: а) $4x \equiv 9 \pmod{13}$; б) $3x \equiv 12 \pmod{15}$; в) $20x \equiv 30 \pmod{55}$.

Задача 2.9. Решите систему сравнений

$$\begin{cases} 6x + 5y \equiv 1 \pmod{11}, \\ 4x + 3y \equiv 2 \pmod{11}. \end{cases}$$

Задача 2.10. а) Докажите, что $(p-2)! \equiv 1 \pmod{p}$ при любом простом p. б) Докажите, что если $(n-2)! \equiv 1 \pmod{n}$, то n — простое.

Задача 2.11. а) Докажите, что если $p = 4k+1$ — простое число, то $x = ((p-1)/2)!$ удовлетворяет сравнению $x^2 \equiv -1 \pmod{p}$. б) Найдите хотя бы одно натуральное решение сравнения $x^2 \equiv -1 \pmod{29}$, не превосходящее 28.

Задача 2.12. С помощью теоремы Вильсона докажите, что среди чисел вида $n! + 1$ бесконечно много составных[1].

Задача 2.13. Пусть $k \geqslant 3$. Найдите все решения сравнения $x^2 \equiv 1 \pmod{2^k}$.

См. также задачи Д19—Д22.

Решения и указания

2.8. а) Найдём остаток, обратный к 4 (mod 13). Для этого перепишем искомое сравнение в виде уравнения $4m - 13n = 1$. Так как $4 \cdot 3 - 13 = -1$, в качестве m можно взять $-3 \equiv 10$. Теперь (см. задачу 2.7в) домножим обе части сравнения на 10: $40x \equiv 90 \pmod{13}$, или $x \equiv 12 \pmod{13}$. Ответ: $x \equiv 12 \pmod{13}$.

б) Так как 3, 12 и 15 имеют НОД, равный 3, на него можно сократить, получив равносильное сравнение $x \equiv 4 \pmod{5}$. Это и есть ответ.

в) Сначала сократим всё (включая 55) на 5, перейдя к сравнению $4x \equiv 6 \pmod{11}$. Теперь сократим $4x$ и 6 ещё

[1] До сих пор неизвестно, конечно ли количество простых чисел вида $n! + 1$ (A038507). Всего известно 22 таких числа (A002981), и наибольшим известным n, дающим простое значение $n! + 1$, является $n = 150209$ (найдено в 2011 г.). Это огромное число содержит 712355 десятичных знаков и входит в список 500 наибольших известных простых чисел (http://primes.utm.edu/primes/lists/short.txt).

на 2: $2x \equiv 3 \pmod{11}$. Осталось заметить, что $1/2 \equiv 6 \pmod{11}$, поэтому решением служит $x \equiv 3 \cdot 6 \pmod{11}$. Ответ: $x \equiv 7 \pmod{11}$.

2.9. Выразим y из первого сравнения и подставим результат во второе: $5y \equiv 1 - 6x$. Так как $5 \cdot 2 \equiv -1$, то $5 \cdot (-2) \equiv 1$, то есть $y \equiv -2(1 - 6x) = 12x - 2 \equiv x - 2$. Подставляем во второе сравнение: $4x + 3(x - 2) \equiv 2$, откуда $7x \equiv 8$. Домножим на -3: $x \equiv -24 \equiv 9 \pmod{11}$. Теперь подставим найденное значение x и получим $y \equiv 7 \pmod{11}$.

2.10. а) По теореме Вильсона

$$(p-1)! = (p-2)!(p-1) \equiv -1 \pmod{p}.$$

Так как $p - 1 \equiv -1 \pmod{p}$, то после домножения на -1 получаем $(p-2)! \equiv 1 \pmod{p}$.

б) Если n имеет простой делитель $1 < p < n$, то и этот делитель, и n/p входят множителями в $(n-2)!$ (так как оба они меньше n, а $(n-1) \perp n$). Тогда $(n-2)!$ сравнимо с 0 по модулю n, значит, предположение о существовании простого делителя неверно, и n — простое число.

2.11. а) Заметим, что

$$(p-1)(p-2)\ldots((p+1)/2) \equiv (-1)(-2)\ldots(-(p-1)/2) = \\ = ((p-1)/2)!(-1)^{2k} = ((p-1)/2)!.$$

Отсюда $(p-1)! \equiv [((p-1)/2)!]^2$. Теперь утверждение задачи получается непосредственным применением теоремы Вильсона.

б) $x \equiv 14! \equiv (2 \cdot 3)(4 \cdot 5)(6 \cdot 7)(8 \cdot 9)(10 \cdot 11)(12 \cdot 13) \cdot 14 \equiv \equiv 6 \cdot (-9) \cdot 13 \cdot 14 \cdot (-6) \cdot 11 \cdot 14 \equiv 4 \cdot 8 \cdot (-8) \cdot 14 = 3 \cdot 4 = = 12$. Осталось возвести в квадрат и проверить: $12^2 = 144 \equiv \equiv -1 \pmod{29}$.

2.12. Если $n + 1$ — простое число, большее 3, то $n! + 1$ делится на него и при этом $n! + 1 > n + 1$, т. е. $n! + 1$ является составным. Так как простых чисел бесконечно много, среди чисел вида $n! + 1$ бесконечно много составных.

2.13. Найдём все $x \leqslant 2^k$, для которых $(x-1)(x+1) \vdots 2^k$. Ясно, что хотя бы один из множителей должен быть чётным. Но так как другой множитель отличается на 2, то он

тоже чётен. А так как НОД$(x-1, x+1)=2$, то одна скобка делится на 2, а вторая кратна 2^{k-1}. Следовательно, здесь возможны 4 случая: 1) $x-1\equiv 0$; 2) $x+1\equiv 0$; 3) $x-1\equiv 2^{k-1}$; 4) $x+1\equiv 2^{k-1}$. Каждый случай даёт своё решение сравнения. Ответ: 1, $2^{k-1}-1$, $2^{k-1}+1$, 2^k-1.

Занятие 3

Леонард Эйлер и его функция

Пусть m — натуральное число. Количество чисел, взаимно простых с m и не больших m, обозначается $\varphi(m)$ и называется *функцией Эйлера*. Значение $\varphi(m)$ равно количеству правильных несократимых дробей со знаменателем m, потому что каждый числитель такой дроби взаимно прост с m. В нотации Айверсона: $\varphi(m) = \sum\limits_{1 \leqslant i \leqslant m} [i \perp m]$.

Приведённой системой остатков по модулю m называется такой набор чисел, в котором все числа взаимно просты с m и любое взаимно простое с m целое число сравнимо ровно с одним числом из набора.

Иначе говоря, приведённая система остатков — это пересечение полной системы и множества чисел, взаимно простых с m. Также заметим, что все приведённые системы остатков содержат одно и то же количество элементов, а именно $\varphi(m)$.

Задача 3.1. Пусть $a \perp m$ и числа $k_1, k_2, \ldots, k_r$ образуют приведённую систему остатков по модулю m. Для каких b числа $ak_i + b$ также образуют приведённую систему остатков по модулю m?

Ответ: необходимо и достаточно, чтобы b делилось на все простые делители числа m.

Доказательство. Необходимость. Так как $a \perp m$, то $-b/a$ — какой-то остаток. Если $b \perp p$ для некоторого p — простого делителя m, то этот остаток взаимно прост с p, а значит, должен совпадать с каким-то из $k_i \pmod p$. Но тогда $ak_i + b \equiv 0 \pmod p$, а следовательно, НОД$(m, ak_i + b) > 1$. Это противоречит тому, что $ak_i + b$ входит в приведённую систему остатков.

Достаточность. Пусть b делится на все простые множители m. Если какое-то из чисел $ak_i + b$ *не* взаимно просто с m, то НОД$(ak_i + b, m) > 1$, то есть делится на некоторое

Леонард Эйлер (1707—1783) — величайший математик XVIII века, ученик Иоганна Бернулли. Большая часть его работ была написана в Санкт-Петербурге и опубликована в академических изданиях Петербургской АН. В теории чисел Эйлер был одним из первых, кто оценил математический гений Пьера Ферма и сумел доказать ряд оставленных им теорем.

Функция Эйлера была впервые использована в 1760 году для доказательства малой теоремы Ферма, а затем и для доказательства более общего утверждения — теоремы Эйлера. Современное обозначение $\varphi(m)$ предложил позднее Гаусс. В западной литературе эту функцию иногда называют «totient function».

простое p. Но $b \vdots p$, поэтому $ak_i \vdots p$, значит, и $k_i \vdots p$, что невозможно для приведённого остатка. А так как умножение на $a \perp m$ и прибавление b — операции обратимые, то они количество остатков не меняют, поэтому $ak_i + b$ — приведённая система остатков.

Задача 3.2. а) Чему равно $\varphi(1)$? б) Чему равно $\varphi(p)$, если p — простое число? в) Докажите, что $\varphi(p^2) = p(p-1)$ для простого p.

Решение. а) $\varphi(1) = 1$, потому что существует ровно одно натуральное число, не большее 1 и взаимно простое с 1.

б) $\varphi(p) = p - 1$, потому что все числа, меньшие простого числа p, взаимно просты с ним. в) Среди натуральных чисел от 1 до p^2 не взаимно простыми с p^2 являются лишь числа, кратные p, то есть p, $2p$, ..., p^2. Этих чисел ровно p, а остальные $p^2 - p$ чисел взаимно просты с p^2. Таким образом, $\varphi(p^2) = p(p - 1)$.

Задача 3.3. Докажите, что $\varphi(p^n) = p^{n-1}(p - 1)$ при любом натуральном n и простом p.

Указание. Решение полностью аналогично решению задачи 3.2в).

Задача 3.4. Докажите, что функция Эйлера *мультипликативна*: при $a \perp b$ выполнено равенство $\varphi(ab) = \varphi(a)\varphi(b)$.

Решение. При $a = 1$ или $b = 1$ эта формула, очевидно, верна. Пусть $a > 1$ и $b > 1$. Расположим числа от 1 до ab в виде таблицы $a \times b$:

1	2	...	r	...	a
$a + 1$	$a + 2$	...	$a + r$	...	$2a$
$2a + 1$	$2a + 2$	...	$2a + r$	...	$3a$
...	...	...	...	...	...
$(b - 1)a + 1$	$(b - 1)a + 2$	...	$(b - 1)a + r$	...	ba

Значение $\varphi(ab)$ равно количеству чисел в этой таблице, взаимно простых с ab. Эти числа должны быть взаимно простыми и с a, и с b. Так как НОД$(qa + r, a)$ = НОД(r, a), то числа в r-м столбце таблицы взаимно просты с a тогда и только тогда, когда число r (то есть число из первой строки этого столбца) взаимно просто с a. Таких столбцов, очевидно, ровно $\varphi(a)$. Осталось выяснить, сколько в таких столбцах чисел, взаимно простых с b. Рассмотрим числа r-го столбца: r, $a + r$, $2a + r$, ..., $(b - 1)a + r$. Среди них нет двух сравнимых по модулю b, т.е. они образуют полную систему остатков по модулю b (см. задачу 1.7в). А значит, среди них ровно $\varphi(b)$ взаимно простых с b. Таким образом, в каждом из $\varphi(a)$ столбцов, в которых существуют взаимно простые с ab числа, таких чисел ровно $\varphi(b)$. Отсюда получаем, что общее их количество равно $\varphi(a)\varphi(b)$.

Задача 3.5. Пусть

$$n = \prod_i p_i^{k_i}$$

— каноническое разложение числа n на простые множители. Выведите из задач 3.3 и 3.4, что

$$\varphi(n) = \prod_i (p_i - 1) p_i^{k_i - 1} = n \prod_i \left(1 - \frac{1}{p_i}\right)$$

(в обоих вариантах формулы произведение берётся по всем простым делителям n).

Указание. Все множители в выписанных произведениях попарно взаимно просты. Для каждого из них применяем результат задачи 3.3, а затем для произведения взаимно простых чисел используем результат задачи 3.4.

Задача 3.6. а) Миша выписал все правильные дроби со знаменателем 30 и привёл их все к несократимому виду. Для каждого знаменателя найдите, сколько дробей с этим знаменателем он получил. Докажите, что $30 = \varphi(1) + \varphi(2) + \varphi(3) + \varphi(5) + \varphi(6) + \varphi(10) + \varphi(15) + \varphi(30)$.

б) **(Тождество Гаусса)** Докажите, что любое натуральное число равно сумме значений функции Эйлера для всех его делителей: $n = \sum\limits_{n:d} \varphi(d) = \sum \varphi(d)[n : d]$.

Решение. а) У Миши получились дроби 1/30, 1/15, 1/10, 2/15, 1/6, 1/5, 7/30, 4/15, 3/10, 1/3, 11/30, 2/5, 13/30, 7/15, 1/2, 8/15, 17/30, 3/5, 19/30, 2/3, 7/10, 11/15, 23/30, 4/5, 5/6, 13/15, 9/10, 14/15, 29/30. Добавим к ним еще дробь $30/30 = 1/1$. Знаменатель 30 остался ровно у тех дробей, у которых числитель был взаимно прост с числом 30, то есть ровно у $\varphi(30) = 8$ дробей, остальные дроби было можно сократить. Все остальные знаменатели получены при сокращении дробей со знаменателем 30, поэтому они являются делителями 30. Докажем, что для любого делителя d после сокращения остались все несократимые правильные дроби со знаменателем d. Для примера рассмотрим $d = 15$. Любая дробь $m/15$ получилась сокращением на 2 из дроби $2m/30$. Значит, у нас есть ровно $\varphi(15) = 8$ дробей со знаменателем 15. Аналогично, знаменатель 10 имеют $\varphi(10) = 4$ дроби, знаменатель 6 имеют $\varphi(6) = 2$ дроби,

знаменатель 5 остался у $\varphi(5) = 4$ дробей, знаменатель 3 — у $\varphi(3) = 2$ дробей. И, наконец, у одной дроби оказался знаменатель 2, а еще у одной — знаменатель 1. Доказываемое равенство следует из того, что общее количество дробей осталось тем же, что и было исходно, то есть 30.

б) Повторите те же самые рассуждения, подставляя вместо 30 произвольное число n.

Задачи для самостоятельного решения

Задача 3.7. Докажите, что $\varphi(m)$ чётно при любом $m > 2$.

Задача 3.8. Докажите, не опираясь на результат задачи 3.5, что: а) $\varphi(m^2) = m\varphi(m)$ для любого натурального m; б) $\varphi(m^k) = m^{k-1}\varphi(m)$ для любых m и k.

Задача 3.9. Докажите, что:

а) $ab = \text{НОД}(a, b)\text{НОК}(a, b)$;

б) $\varphi(a)\varphi(b) = \varphi(\text{НОД}(a, b))\varphi(\text{НОК}(a, b))$;

в) $\varphi(ab)\varphi(\text{НОД}(a, b)) = \varphi(a)\varphi(b)\text{НОД}(a, b)$.

Задача 3.10. Используя формулу для функции Эйлера из задачи 3.4, докажите, что простых чисел бесконечно много.

Задача 3.11. Докажите, что $\varphi(n) = n/2$ тогда и только тогда, когда n — степень двойки.

Задача 3.12. Докажите, что если $n \vdots d$, то $\varphi(n) \vdots \varphi(d)$.

См. также задачи Д23—Д36.

Решения и указания

3.7. Указание. Разберите два случая: 1) m — степень двойки; 2) m имеет нечётный простой делитель p.

3.8. Указание. а) Взаимно простыми с m^2 являются те и только те числа, которые взаимно просты с m. На каждом из m отрезков $[1; m]$, $[m + 1, 2m]$, ..., $[(m - 1)m + 1, m^2]$ таких чисел ровно $\varphi(m)$, потому что целые числа из каждого такого отрезка образуют полную систему остатков по модулю m. б) Доказывается аналогично, с помощью разбиения на отрезки, только отрезков теперь m^{k-1}.

3.9. а) Будем обозначать через $\text{ord}_p a$ наибольшую степень простого числа p, на которую делится a. Если $\text{ord}_p a = k$,

а $\operatorname{ord}_p b = l$, то $\operatorname{ord}_p \text{НОД}(a, b) = \min(k, l)$, а $\operatorname{ord}_p \text{НОК}(a, b) = \max(k, l)$. Так как при перемножении степени складываются, а $\min(k, l) + \max(k, l) = k + l$, то левая и правая части равенства делятся на одну и ту же степень простого числа p, и это верно для каждого p.

б) Пусть $p_1, p_2, \ldots$ — простые числа, делящие a, но не делящие b; $q_1, q_2, \ldots$ — простые числа, делящие b, но не делящие a; $r_1, r_2, \ldots$ — простые числа, делящие и a, и b. Обозначим

$$P = \prod_i \left(1 - \frac{1}{p_i}\right), \quad Q = \prod_i \left(1 - \frac{1}{q_i}\right), \quad R = \prod_i \left(1 - \frac{1}{r_i}\right).$$

Тогда $\varphi(a) = aPR$, $\varphi(b) = bQR$, $\varphi(\text{НОД}(a, b)) = \text{НОД}(a, b)R$, $\varphi(\text{НОК}(a, b)) = \text{НОК}(a, b)PQR$. С учётом тождества из пункта а) сразу получаем требуемое.

в) Пусть, как и в предыдущем пункте, $p_1, p_2, \ldots$ — простые числа, делящие a, но не делящие b; $q_1, q_2, \ldots$ — простые числа, делящие b, но не делящие a; $r_1, r_2, \ldots$ — простые числа, делящие и a, и b,

$$P = \prod_i \left(1 - \frac{1}{p_i}\right), \quad Q = \prod_i \left(1 - \frac{1}{q_i}\right), \quad R = \prod_i \left(1 - \frac{1}{r_i}\right).$$

Тогда $\varphi(ab) = abPQR = (aPR)(bQR)/R = \varphi(a)\varphi(b)/R$. Осталось заметить, что $\varphi(\text{НОД}(a, b)) = \text{НОД}(a, b) \cdot R$, то есть $R = \varphi(\text{НОД}(a, b))/\text{НОД}(a, b)$.

Комментарий. Из задачи 3.9в следует, что

$$\varphi(ab) > \varphi(a)\varphi(b),$$

если $\text{НОД}(a, b) > 1$.

3.10. Предположим противное и рассмотрим число N, равное произведению всех (конечного числа!) различных простых чисел. Тогда натуральные числа, меньшие N, кроме числа 1, не могут быть взаимно простыми с ним, поскольку каждое натуральное число делится хотя бы на один из простых множителей, а N делится на каждый из них. Это значит, что $\varphi(N) = 1$. Но это противоречит формуле

$$\varphi(p_1 p_2 \ldots p_k) = (p_1 - 1)(p_2 - 1)\ldots(p_k - 1),$$

потому что в её правой части стоит число, большее 1.

3.11. В сторону «тогда» утверждение следует из задачи 3.8б при $m = 2$. Докажем его в обратную сторону тремя разными способами.

Решение 1. По условию n четно. Значит, взаимно простыми с ним могут быть только нечётные числа. Поскольку нечетных чисел от 1 до n всего $n/2$, а $\varphi(n) = n/2$, каждое нечётное число взаимно просто с n. Значит, у n нет нечётных делителей.

Решение 2. Из формулы

$$\varphi(n) = n \prod_i \left(1 - \frac{1}{p_i}\right)$$

получается, что $\varphi(n)/n$ равно произведению тех из дробей $1/2$, $2/3$, $4/5$, $6/7$, знаменатели которых являются простыми делителями n. Если среди этих дробей есть $1/2$, то никаких других дробей быть не может, потому что иначе произведение будет меньше $1/2$. (И это значит, что единственным простым множителем n является двойка, то есть n — степень 2). Если же $1/2$ среди этих дробей отсутствует, то произведение дробей имеет чётный числитель и нечётный знаменатель, то есть не может быть равным $1/2$.

Решение 3 (с помощью тождества Гаусса). Согласно тождеству Гаусса, $n = \sum \varphi(d)[n \vdots d]$. Выделим из всей суммы одно слагаемое $\varphi(n) = n/2$. Вычтя его из обеих частей, получим $n/2 = \sum \varphi(d)[n \vdots d][d < n]$ (в формулах мы воспользовались «скобками Айверсона», см. с. 4).

Но тождество Гаусса для $n/2$ говорит, что $n/2$ равно сумме $\varphi(d)$ по всем делителям числа $n/2$ (естественно, не большим $n/2$). А так как каждый делитель числа $n/2$ (автоматически!) является делителем n, сравнение двух равенств позволяет сделать очень простой вывод: среди делителей числа n, меньших n, нет таких, которые бы не были делителями $n/2$. На первый взгляд кажется, что такое невозможно: ведь если $m = \mathrm{ord}_2(n)$ (то есть $n \vdots 2^m$, но n не делится на 2^{m+1}), то 2^m как раз и является примером такого делителя числа n, который не делит $n/2$. Кажущееся противоречие устраняется, тем не менее, просто: в случае $n = 2^m$ этот делитель равен n, а не меньше n, а $\varphi(n)$ мы уже раньше вычли

из обеих частей равенства. Таким образом, мы доказали, что $n = 2^m$.

3.12. Воспользуемся формулой

$$\varphi(n) = n \prod_i \left(1 - \frac{1}{p_i}\right)$$

Такую же формулу выпишем для d:

$$\varphi(d) = d \prod_i \left(1 - \frac{1}{q_i}\right)$$

Разделив одно равенство на другое, получим, что

$$\frac{\varphi(n)}{\varphi(d)} = \frac{n}{d} \prod_i \left(1 - \frac{1}{r_i}\right),$$

где в произведении остались только те простые числа r_i, которые делят n, но не делят d. Именно они входят в разложение n/d. Это значит, что $\varphi(n)/\varphi(d)$ кратно

$$\prod_i r_i \cdot \prod_i \left(1 - \frac{1}{r_i}\right) = \prod_i (r_i - 1).$$

Последнее выражение, очевидно, является целым числом.

Занятие 4

КТО-КТО в теремочке живёт

Пусть даны n попарно взаимно простых чисел $m_1, m_2, \ldots, m_n$ и n чисел $r_1, r_2, \ldots, r_n$, для которых $0 \leqslant r_i \leqslant m_i - 1$ при всех $i = 1, 2, \ldots, n$. Числа $r_1, r_2, \ldots, r_n$ мы будем называть *набором остатков*, а произведение $m_1 m_2 \ldots m_n$ обозначим M. Центральное место в сегодняшнем занятии занимает следующая

Китайская теорема об остатках («КТО»). Существует единственное число N, для которого $0 \leqslant N \leqslant M - 1$ и $N \equiv r_i \pmod{m_i}$ для всех $i = 1, 2, \ldots, n$.

Доказательство этой теоремы опирается на такие несложные утверждения.

1) Количество различных наборов остатков равно M.

2) Каждому натуральному числу соответствует какой-то свой набор остатков.

3) Если двум различным натуральным числам соответствуют одинаковые наборы остатков, то разность этих чисел делится на M.

Из утверждений 1)—3) следует, что все наборы остатков, соответствующих числам от 0 до $M - 1$, попарно различны, то есть каждый набор соответствует какому-то одному числу.

К сожалению, это доказательство не даёт ответа на вопрос о способе вычисления числа N. Один из способов будет продемонстрирован после изучения теоремы Эйлера (см. задачу Д49), другие варианты рассмотрены в решении задачи 4.3.

Задача 4.1. Докажите, что для любых попарно взаимно простых чисел $m_1, m_2, \ldots, m_n$ и остатков $r_1, r_2, \ldots, r_n$ по модулям $m_1, m_2, \ldots, m_n$ найдутся n последовательных чисел $a, a + 1, \ldots, a + n - 1$, для которых $a \equiv r_1 \pmod{m_1}$, $a + 1 \equiv r_2 \pmod{m_2}$, $\ldots$, $a + n - 1 \equiv r_n \pmod{m_n}$.


孫子算經卷上

度之所起起於忽欲知其忽纖吐絲爲忽十忽爲一絲十絲爲一毫十毫爲一釐十釐爲一分十分爲一寸十寸爲一尺十尺爲一丈十丈爲一引五十尺爲一端四十尺爲一疋六尺爲一步二百四十步爲一畝三百步爲一里

稱之所起起於秉十秉爲一斛十斛爲一鉄二十四鉄爲一兩十六兩爲一斤三十斤爲一鈞

Страница из «Сунь Цзы Суань Цзин», трактата китайского математика и астронома **Сунь Цзы** (ок. 400 — ок. 460). В этом трактате он впервые привёл задачу, являющуюся частным случаем китайской теоремы об остатках (КТО), и указал способ ее решения.

Указание. Число a должно давать остаток r_1 по модулю m_1, остаток $r_2 - 1$ по модулю m_2, ..., остаток $r_n - n + 1$ по модулю m_n. Осталось воспользоваться КТО.

Задача 4.2. Докажите, что для любого n найдутся n последовательных чисел, делящихся на полные квадраты (отличные от единицы).

Решение. Применим результат задачи 4.1 к набору чисел $m_1 = 2^2$, $m_2 = 3^2$, ..., $m_n = p^2$ (m_n — квадрат n-го простого числа) и набору нулевых остатков.

Задача 4.3. Натуральное число даёт остаток 3 при делении на 5 и остаток 2 при делении на 7. Какой остаток может оно давать при делении на 35?

Ответ: 23.

Решение 1. В силу КТО этот остаток определён однозначно. Чтобы его определить, достаточно выписать все числа от 1 до 35, дающие остаток 2 при делении на 7 (то есть числа 2, 9, 16, 23, 30) и выбрать из них то, которое даёт остаток 3 при делении на 5 — очевидно, что это 23.

Решение 2. Мы ищем числа, одновременно представимые в виде $2 + 7k$ и $3 + 5l$ для натуральных k и l. Это означает, что мы должны научиться решать диофантово уравнение $2 + 7k = 3 + 5l$. Перепишем его в виде $7k - 5l = 1$ и затем решим с помощью алгоритма Евклида[1]. Получим $k = 3$, $l = 4$. Поскольку $2 + 7k = 23$ и $23 < 35$, то мы нашли остаток при делении на 35.

Комментарий: наиболее эффективным является второе решение, опирающееся на алгоритм Евклида. Если необходимо решать систему из нескольких (более чем двух) сравнений, то они решаются последовательно: надо шаг за шагом преобразовывать два сравнения в одно, тем самым уменьшая число оставшихся сравнений на 1.

Задача 4.4. Пятнадцать простых чисел образуют арифметическую прогрессию с положительной разностью d. Докажите, что $d > 30000$.

Решение. Обозначим члены прогрессии $a_1, a_2, \ldots, a_{15}$. Сначала докажем, что d делится на 7. Предположим противное — $d \perp 7$. Тогда из результата задачи 1.7в следует, что числа $a_8, a_9, \ldots, a_{14}$ образуют полную систему остатков при делении на 7, то есть одно из них кратно 7. Так как все эти числа, очевидно, больше 7, то мы получили противоречие с простотой членов прогрессии. Следовательно, d делится на 7, откуда $a_3 \geqslant 15$. Рассмотрим теперь 13 членов прогрессии, начиная с a_3. Снова воспользуемся результатом задачи 1.7в, чтобы доказать, что d делится также на 2, 3, 5, 11 и 13. Следовательно, d делится на произведение $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 = 30030$ и поэтому больше, чем 30000.

Задача 4.5. В китайском календаре используется 12-летний цикл, причём каждому из 12 лет в цикле соответствует одно из животных. Кроме того, каждый год проходит

[1]См. основную лемму занятия 6 в книге ДПЧ.

под покровительством одной из пяти стихий и считается окрашенным в цвет этой стихии: годы, оканчивающиеся на 0 и 1, — годы металла (белый цвет), на 2 и 3 — воды (чёрный или синий), на 4 и 5 — дерева (зелёный или бирюзовый), на 6 и 7 — огня (красный), а на 8 и 9 — земли (жёлтый). Таким образом, за 60 лет каждое животное встречается 5 раз, а каждый цвет — 12 раз. Докажите, что в 60-летнем цикле (гань-чжи) возникают все возможные комбинации животных и цветов.

Решение. Рассмотрим отдельно чётные и нечётные годы (годам каждой чётности соответствует по 6 различных животных, и при этом как среди чётных, так и среди нечётных годов встречаются все цвета). Цвет года среди годов данной чётности повторяется с периодом 5, а животное среди годов данной чётности повторяется с периодом 6. Поскольку 5 и 6 взаимно просты, по КТО для каждой пары остатков существует число, не превосходящее 30 и дающее ровно эту пару остатков. Таким образом, нечётные годы дают все 30 возможных комбинаций цветов с «нечётными животными», а чётные годы — все 30 возможных комбинаций цветов с «чётными животными».

Задача 4.6. Докажите, что числа натурального ряда можно переставить местами так, чтобы сумма любых n первых чисел делилась на n.

Решение 1. Начинаем с единицы. На каждом следующем шаге либо ставим наименьшее неиспользованное число A (если сумма первых n чисел при этом окажется кратной n), либо такое (не использованное ранее в последовательности) число, чтобы сумма n первых делилась на n и была сравнима с $(n + 1 - A)$ по модулю $(n + 1)$. По КТО число, удовлетворяющее двум этим сравнениям, существует. После этого число A можно ставить на следующее место.

Этот алгоритм даёт последовательность 1, 3, 2, 10, 4, 52, 5, ...

Решение 2. Искомую перестановку можно задать «жадным алгоритмом», каждый раз выбирая наименьшее из неиспользованных чисел, для которого среднее арифметическое первых n чисел является целым числом. Резуль-

тат — последовательность 1, 3, 2, 6, 8, 4, 11, 5, 14, 16, 7, ... (A019444).

Комментарий. Любопытнейшим свойством этой последовательности является то, что все циклы в перестановке натурального ряда имеют длину 2: $a(a(n))=n$.

Задачи для самостоятельного решения

Задача 4.7. Докажите, что если натуральный ряд представлен в виде объединения нескольких непересекающихся арифметических прогрессий, то разности любых двух прогрессий имеют общий делитель, больший 1.

Задача 4.8. Найдите наименьшее натуральное число, которое при делении на 3 дает остаток 2, при делении на 5 — остаток 3, при делении на 7 — остаток 2, при делении на 11 — остаток 6.

Задача 4.9. Пусть $f(x)$ — многочлен с целыми коэффициентами. Для $m \geqslant 1$ обозначим через $N_f(m)$ количество различных решений сравнения $f(x) \equiv 0 \pmod{m}$ (решения, отличающиеся на величины, кратные m, будем считать одинаковыми). Докажите, что функция N_f мультипликативна, т. е.

$$N_f(m_1 m_2) = N_f(m_1) N_f(m_2),$$

если $m_1 \perp m_2$.

Задача 4.10. Найдите наименьшее натуральное число, половина которого — квадрат, треть — куб, а пятая часть — пятая степень.

Задача 4.11. При изготовлении елочной гирлянды электрик Петров сделал на куске провода отметки, делящие его на 113 одинаковых кусков, и ушел домой. На следующий день электрик Иванов разметил тот же провод на 137 одинаковых кусков. Наконец, электрик Сидоров разрезал провод по всем отметкам. Куски какого размера у него получились и сколько получилось кусков каждого вида?

Задача 4.12. Докажите, что если бы Сидоров разрезал провод на 250 одинаковых кусков, то на каждом из получившихся кусочков, кроме двух крайних, стояло бы ровно по одной отметке.

Решения и указания

4.7. Рассмотрим две прогрессии со взаимно простыми разностями m и n. Пусть A_1 и A_2 ($A_1 > A_2$) — первые члены этих прогрессий. Тогда среди членов второй прогрессии на отрезке $[A_1; A_1 + mn]$ встретятся все остатки при делении на m, а значит, и нулевой. Таким образом, две такие прогрессии всегда пересекаются.

4.8. Ответ: 1073.

4.9. Для любого многочлена с целыми коэффициентами и любой пары целых чисел x, y разность $f(x + y) - f(x)$ делится на y. Пусть x — произвольное решение сравнения $f(x) \equiv 0 \pmod{m}$, m_1 — делитель m, а r_1 — остаток от деления x на m_1. Тогда $x = m_1q_1 + r_1$, $f(m_1q_1 + r_1) - f(r_1)$ делится на m_1. Мы получили, что r_1 — решение сравнения $f(r_1) \equiv 0 \pmod{m_1}$. Аналогично из того же произвольного решения x построим решение r_2 для m_2. Мы получили, что каждому решению x соответствует пара решений (r_1,r_2) для сравнений по модулям m_1 и m_2 соответственно. Но согласно КТО, любая пара остатков (r_1,r_2) при $m = m_1m_2$ и $m_1 \perp m_2$ однозначно (по модулю m) задаёт число x, дающее такую пару остатков, и разным таким парам соответствуют различные x. Это означает, что по паре решений (r_1,r_2) однозначно восстанавливается x. Осталось убедиться, что $f(x) = f(m_1q_1 + r_1) = f(r_1) \equiv 0 \pmod{m_1}$ и $f(x) \equiv 0 \pmod{m_2}$, поэтому $f(x) \equiv 0 \pmod{m_1m_2}$. Построенное взаимно однозначное соответствие и доказывает мультипликативность функции N_f.

4.10. Из условия следует, что искомое число n делится на 2, 3 и 5. При этом показатель степени 2 в разложении n на простые множители (это число обозначается $\mathrm{ord}_2(n)$ — см. решение задачи 3.9) должен быть сравним с 1 (mod 2), 0 (mod 3) и 0 (mod 5). Наименьшим таким показателем является 15. Аналогично, $\mathrm{ord}_3(n)$ должен быть 1 (mod 3), 0 (mod 2) и 0 (mod 5), наименьший показатель равен 10. Наименьшим возможным $\mathrm{ord}_5(n)$ является 6. Ясно, что наличие других простых делителей только увеличит число. Ответ: $2^{15} \cdot 3^{10} \cdot 5^6$.

4.11. Всего получилось $113 + 137 - 1 = 249$ кусков. Их длины кратны $E = 1/(113 \cdot 137)$ и не больше, чем $1/137 = 113E$. Согласно КТО, кусков размера E, $2E$, $3E$, ..., $112E$ будет по 2. Кусков размера $1/137$ должно остаться $137 - 112 = 25$, потому что именно на таком количестве кусков Иванова не было отметок, сделанных Петровым.

4.12. Между любыми двумя дробями $a/137$ и $b/113$ находится их медианта — дробь $(a + b)/(113 + 137)$. Это означает, что ни на каком из 250 кусков не может быть двух отметок. Но так как отметок всего 248, а два крайних куска пусты, то на каждом из остальных кусков хотя бы одна отметка должна быть.

Занятие 5

От Ферма к Эйлеру и обратно

Задача 5.1. а) Докажите, что если p — простое число и $0 < a < p$, то $a \cdot 2a \cdot 3a \cdot \ldots \cdot (p-1)a \equiv (p-1)! \pmod{p}$.

б) **(Малая теорема Ферма, МТФ)** Докажите, что если p — простое число и $a \perp p$, то $a^{p-1} \equiv 1 \pmod{p}$.

Решение. а) Достаточно доказать, что среди чисел a, $2a$, ..., $(p-1)a$ по модулю p нет одинаковых. Это мы уже делали выше (в ответе на вопрос 2 занятия 1). Отсюда следует, что эти числа — какая-то перестановка чисел $1, 2, \ldots, p-1$. Но тогда мы знаем, чему равно их произведение.

б) В левой части сравнения а) стоит $(p-1)!a^{p-1}$, а в правой — просто $(p-1)!$. Поскольку все положительные числа, меньшие простого числа p, взаимно просты с ним, а произведение нескольких взаимно простых также будет взаимно простым, получаем, что $p \perp (p-1)!$. Это позволяет сократить обе части сравнения на $(p-1)!$. В результате получается утверждение МТФ.

Лемма. Пусть $a \perp n$ и $a_1, a_2, \ldots, a_k$ — положительные числа, меньшие n и взаимно простые с n (разумеется, $k = \varphi(n)$). Тогда совокупность остатков от деления $aa_1, aa_2, \ldots, aa_k$ на n — какая-то перестановка тех же самых чисел.

Доказательство. Докажем, что сравнение $aa_i \equiv aa_j \pmod{n}$ невозможно при различных i и j. Это следует из условия $a \perp n$ (см. задачу 1.7). Но тогда для каждого i существует какое-то b, для которого $aa_i \equiv b_i \pmod{n}$, причём $b_i \perp n$ как произведение двух чисел, взаимно простых с n, и для разных i эти b_i будут разными. Следовательно, набор $b_1, b_2, \ldots, b_k$ представляет перестановку чисел $a_1, a_2, \ldots, a_k$.

Теорема Эйлера. Если НОД$(a, n) = 1$, то $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Доказательство. Перемножив все сравнения $aa_i \equiv b_i \pmod{n}$ и сократив результат на произведение $a_1a_2\ldots a_k = b_1b_2\ldots b_k$, взаимно простое с n, получим требуемое.

Комментарий. Если n простое, то в качестве следствия из теоремы Эйлера получаем МТФ.

Задача 5.2. Пусть p простое. Докажите, что если $a^p \equiv b^p \pmod p$, то а) $a \equiv b \pmod p$; б) $a^p \equiv b^p \pmod{p^2}$.

Решение. а) Для сравнения по модулю p:

$$a \equiv a^p \text{ (по МТФ)} \equiv b^p \text{ (по условию)} \equiv b \text{ (по МТФ)}.$$

б) В силу пункта а), $a = b + kp$ для некоторого целого k. Тогда $a^p - b^p = (b + kp)^p - b^p$. Если раскрыть скобки по формуле бинома Ньютона, то все слагаемые, начиная с третьего, будут кратны p^2. Из первых двух слагаемых $b^p + pb^{p-1}kp$ второе тоже кратно p^2, а первое затем вычитается.

Задача 5.3. Пусть p простое. Если $m \equiv 1 \pmod{p^d}$, то $m^p \equiv 1 \pmod{p^{d+1}}$.

Указание. Аналогично задаче 5.2б, $m^p = (1 + kp^d)^p$ для некоторого k, и после возведения в степень выяснится, что все слагаемые, начиная с третьего, делятся на p^{2d}, а второе делится на p^{d+1}. Следовательно, всё выражение даёт остаток 1 по модулю p^{d+1}.

Комментарий. Эта задача даёт путь к другому доказательству теоремы Эйлера. Пусть $n = \prod\limits_i p_i^{k_i}$ — каноническое разложение числа n на простые множители. Тогда

$$\varphi(n) = \prod_i (p_i - 1)p_i^{k_i - 1}.$$

Из задачи 5.3 и МТФ следует, что

$$a^{(p_i-1)p_i^{k_i-1}}.$$

Следовательно,

$$a^{\varphi(n)} \equiv 1 \pmod{p_i^{k_i}}.$$

Отсюда

$$a^{\varphi(n)} \equiv 1 \pmod n.$$

Задача 5.4 (продолжение задачи 5.3). Если $a^n - b^n$ делится на n, то $(a^n - b^n)/(a - b)$ делится на n.

Указание. Разложите n на простые множители и докажите утверждение задачи отдельно для каждого простого множителя, входящего (в некоторой степени) в разложение n.

Пьер де Ферма́ (1601—1665) — французский математик, один из создателей теории чисел. Вёл активную переписку со всеми крупнейшими математиками своего времени. Именно в этой переписке им были сформулированы многие его открытия. Наиболее известна Великая теорема Ферма, доказанная только в самом конце XX века.

Утверждение, которое ныне называют малой теоремой Ферма, было сформулировано без доказательства в письме к Пьеру Френикл ю от 18 октября 1640 года. Первые доказательства, полученные Лейбницем и Эйлером, были достаточно сложны. Доказательство, приведенное в этом занятии, принадлежит шотландскому математику Джеймсу Айвори и опубликовано им в 1806 году.

Задача 5.5. Пусть p — простое число. Докажите, не опираясь на МТФ, что если $m^p \equiv m \pmod{p}$, то $(m+1)^p \equiv (m+1) \pmod{p}$.

Решение. Имеем $(m+1)^p \equiv m^p + 1 \pmod{p}$, так как левая часть равна сумме $C_p^k m^k$, и каждый биномиальный коэффициент, кроме двух крайних, делится на p. А так как $m^p \equiv m$, то $(m+1)^p \equiv m^p + 1 \equiv m + 1$.

Задача 5.6. Пусть p — простое число.

а) **(Тождество Эйзенштейна)** Докажите, что

$$(a+b)^p - a^p - b^p \vdots p.$$

б) Докажите, что $(a_1 + a_2 + ... + a_n)^p - a_1^p - a_2^p - ... - a_n^p \vdots p$.

Комментарий. Задачи 5.5 и 5.6б дают еще два способа доказательства МТФ (в 5.5 фактически доказан индукционный переход, необходимый для доказательства МТФ индукцией по m, а в 5.6б нужно приравнять все переменные единице).

Показателем (или *мультипликативным порядком*) числа a по модулю m называется наименьшее натуральное l, для которого $a^l \equiv 1 \pmod{m}$.

Из теоремы Эйлера следует, что показатель любого числа не больше $\varphi(m)$. Те числа, показатель которых равен $\varphi(m)$ (если они есть), называются *первообразными корнями* по модулю m.

Задачи для самостоятельного решения

Задача 5.7. Найдите остаток от деления а) 2^{100} на 101; б) 2^{900} на 29; в) 28! на 29; г) 56!! на 29.

Задача 5.8. Пусть p — простое число, большее 5. Докажите, что число 11111...11 ($p-1$ единица) делится на p.

Задача 5.9. Докажите, что $16^{2n+1} + (2n+1)^{16} \vdots 17$, если $(2n+1) \perp 17$.

Задача 5.10. Докажите, что если $n \perp 19$, то либо $n^9 + 1 \vdots 19$, либо $n^9 - 1 \vdots 19$.

Задача 5.11. Докажите, что если $n \perp 17$, то одно из чисел n^8+1, n^4+1, n^2+1, $n+1$, $n-1$ делится на 17.

Задача 5.12. Докажите, что $17^{120} - 1 \vdots 143$.

См. также задачи Д37—Д48.

Решения и указания

5.7. а) Так как 101 — простое число, по МТФ имеем $2^{100} \equiv 1 \pmod{101}$.

б) Вместо того чтобы считать длину цикла остатков, как это делалось в первом занятии, воспользуемся МТФ. Так

как 29 — простое число, $2^{28} \equiv 1 \pmod{29}$. Разделим 900 на 28 с остатком: $900 = 32 \cdot 28 + 4$. Поэтому $2^{900} = 2^{28 \cdot 32 + 4} \equiv$ $\equiv 2^4 \pmod{29} = 16$.

в) -1 (по теореме Вильсона).

г) $56!! = 2^{28} \cdot 28! \equiv 1 \cdot (-1) \equiv -1 \pmod{29}$.

5.8. $11111...11 = (10^{p-1} - 1)/9$. Число $10^{p-1} - 1$ делится на p по МТФ. Поскольку $p \neq 3$, $1/9$ от этого числа тоже делится на p.

5.9. $16^{2n+1} + (2n+1)^{16} \equiv (-1)^{2n+1} + (2n+1)^{16} \equiv -1 + 1 \equiv$ $\equiv 0 \pmod{17}$.

5.10. $n^{18} \equiv 1$ по МТФ. Осталось заметить, что $n^{18} - 1 =$ $= (n^9 + 1)(n^9 - 1)$, поэтому хотя бы один из множителей делится на 19.

5.11. Аналогично предыдущей задаче, применить МТФ и затем воспользоваться тождеством

$$n^{16} - 1 = (n^8 + 1)(n^4 + 1)(n^2 + 1)(n + 1)(n - 1).$$

5.12. Воспользоваться тем, что $n^{12} - 1 \vdots 13$ при $n = 17^{10}$ и $n^{10} - 1 \vdots 11$ при $n = 17^{12}$.

Занятие 6

Псевдопростые числа и числа Кармайкла

Пусть дано некоторое нечётное число n, про которое мы хотим узнать, является оно простым или составным. Если n невелико, мы можем просто делить его на все нечётные числа, не превосходящие $\sqrt{n}$. Если при этом найдётся делитель, то n составное, иначе n простое.

Однако для больших n этот метод очень трудоёмок, так что стоит поискать более эффективные способы определения простоты числа n. Одним из таких способов служит использование МТФ, согласно которой $a^{n-1} \equiv 1 \pmod{n}$ для простого n. Следовательно, если мы обнаруживаем, что a^{n-1} не сравнимо с 1 по модулю n, то n составное. Таким образом, для каждого значения a получается свой *тест Ферма* проверки числа на простоту — необходимое условие простоты числа n. Чаще всего тест Ферма используется для $a = 2$.

Пусть, например, мы проверяем простоту числа 851 и для этого хотим вычислить 2^{850} по модулю 851. Двоичное разложение числа 850 имеет вид $2^1 + 2^4 + 2^6 + 2^8 + 2^9$. Последовательно возводя в квадрат (как в решении задачи Д14), находим

$$2^2 = 4, \quad 2^4 = 16, \quad 2^8 = 256, \quad 2^{16} \equiv 9, \quad 2^{32} \equiv 81,$$
$$2^{64} \equiv 604, \quad 2^{128} \equiv 588, \quad 2^{256} \equiv 238, \quad 2^{512} \equiv 478.$$

Теперь, перемножая 4, 9, 604, 238 и 478 по модулю 851, получаем 169, а не 1. Это означает, что 851 не является простым (и действительно, $851 = 30^2 - 7^2 = 23 \cdot 37$).

Тест Ферма позволяет установить, что число является составным, но не позволяет доказать простоту числа.

Составное число n, для которого $2^n \equiv 2 \pmod{n}$, называется *псевдопростым по основанию* 2. Аналогично можно определить псевдопростые числа по другим основаниям.

Роберт Дэниэл Кармайкл (1879—1967) — американский математик. Наиболее известен вкладом в теорию чисел. Например, одна из теорем Кармайкла утверждает, что n-е число Фибоначчи при любом $n > 12$ имеет простой делитель, который не делит ни одно из предыдущих чисел Фибоначчи. Другая теорема касается функции Кармайкла $\lambda(n)$ — наименьшего значения показателя степени, для которого при любом $a > 1$ и $a \perp n$ выполнено сравнение $a^{\lambda(n)} \equiv 1 \pmod{n}$. А именно, утверждается, что $\lambda(n) = \varphi(n)$ для всех степеней нечётных простых и удвоенных степеней нечётных простых чисел, а также для $n = 2$ и $n = 4$.

Последовательность псевдопростых по основанию 2 — A001567 (их также называют числами Сарруса[1]), по основанию 3 — A005935, по основанию 5 — A005936.

Задача 6.1. Примените тест Ферма для проверки на простоту чисел 511 и 509.

---

[1]В честь Фредерика Сарруса, открывшего в 1819 году, что число 341 является контрпримером к «китайской гипотезе», согласно которой все числа, прошедшие тест Ферма по модулю 2, — простые.

Решение. Имеем $2^9 \equiv 1 \pmod{511}$, поэтому $2^{511} \equiv 2^{9\cdot 56+7} \equiv$ $\equiv 2^7 \not\equiv 2 \pmod{511}$. Поэтому 511 заведомо не является простым.

Далее, $2^9 \equiv 3 \pmod{509}$, поэтому $2^{509} = 2^{9\cdot 56+5} \equiv 3^{56}2^5$. Так как $3^7 = 2187 \equiv 151$, $151 \cdot 151 \equiv 405$, $405 \cdot 405 \equiv 127$, $127 \cdot 127 \equiv 350$, а $350 \cdot 32 \equiv 2$ (все сравнения — по модулю 509), получаем, что 509 проходит 2-тест Ферма. Это не позволяет ничего сказать о простоте числа 509.

Комментарий: $511 = 7 \cdot 73$, а число 509 на самом деле простое.

Задача 6.2. Докажите, что если p и q — различные простые числа, то из $a^p \equiv a \pmod{q}$ и $a^q \equiv a \pmod{p}$ следует, что $a^{pq} \equiv a \pmod{pq}$.

Решение. По МТФ $(a^q)^p \equiv a^q \pmod{p}$. По условию $a^q \equiv$ $\equiv a \pmod{p}$. Следовательно, $a^{pq} - a$ делится на p. Аналогично, $a^{pq} - a$ делится на q. Так как p и q простые, то $a^{pq} - a$ делится на их произведение pq.

Задача 6.3. Докажите, что $2^{341} \equiv 2 \pmod{341}$ (при этом $341 = 11 \cdot 31$ — составное число).

Решение. В силу задачи 6.2 достаточно убедиться, что $2^{11} \equiv 2 \pmod{31}$ и $2^{31} \equiv 2 \pmod{11}$. Первое следует из сравнения $2^5 = 32 \equiv 1 \pmod{31}$, второе — из сравнения $2^{10} \equiv 1 \pmod{11}$, справедливого по МТФ.

Верно ли, что для любого составного числа его «непростоту» можно доказать с помощью какого-то теста Ферма (при правильно выбранном основании a)? Как ни удивительно, ответ на этот вопрос отрицателен: существуют составные числа, проходящие тест Ферма по всем простым модулям. Такие числа называют *числами Кармайкла*, или *абсолютно псевдопростыми*.

Задача 6.4. а) **(Теорема Корсельта)** Докажите, что если $n = p_1p_2...p_k$ и $n - 1$ делится на $p_i - 1$ для любого $i = 1, ..., k$, то n — число Кармайкла, т. е. для любого a выполнено сравнение $a^n \equiv a \pmod{n}$.

б) Докажите, что $561 = 3 \cdot 11 \cdot 17$ — число Кармайкла.

в) Докажите теорему, обратную теореме Корсельта.

Комментарий. Из обратной теоремы Корсельта следует, что все числа Кармайкла нечётны: если бы существовало

чётное число Кармайкла n, то для любого его нечётного простого делителя p_1 нечётное число $n-1$ должно было бы делиться на чётное p_1-1.

Задача 6.5. Докажите, что: а) 91 — псевдопростое по основанию 3; б) 217 — псевдопростое по основанию 5; в) 645 — псевдопростое по основанию 2; г) 1729 — псевдопростое по основаниям 2, 3 и 5.

Решение. а) $3^{91} \equiv 3 \pmod{91}$, потому что $91 = 7 \cdot 13$, $90 = 2 \cdot 3^2 \cdot 5$, $3^6 \equiv 1 \pmod 7$ по МТФ и $3^3 = 27 \equiv 1 \pmod{13}$. То есть 3^{90} сравнимо с 1 и по модулю 7, и по модулю 13.

б) $5^{217} \equiv 5 \pmod{217}$, потому что $217 = 7 \cdot 31$, $216 = 6^3$, $5^6 \equiv 1 \pmod 7$ по МТФ, $5^3 = 125 \equiv 1 \pmod{31}$. То есть 5^{216} сравнимо с 1 и по модулю 7, и по модулю 31.

в) Убедимся, что $2^{644} \equiv 1 \pmod{645}$. Так как $645 = 3 \cdot 5 \cdot 43$ и $644 = 2^2 \cdot 7 \cdot 23$, то

$$2^{644} = 4^{2 \cdot 7 \cdot 23} \equiv 1 \pmod 3,$$

$$2^{644} = 16^{7 \cdot 23} \equiv 1 \pmod 5$$

и

$$2^{644} = 128^{4 \cdot 23} \equiv (-1)^{4 \cdot 23} \equiv 1 \pmod{43}.$$

Поэтому $2^{644} \equiv 1 \pmod{3 \cdot 5 \cdot 43}$.

г) Докажем сразу для любого модуля, взаимно простого с 1729: $1729 = 7 \cdot 13 \cdot 19$, $1728 = 12^3 = 2^6 \cdot 3^3$. По МТФ $a^{36} \equiv 1 \pmod{7 \cdot 13 \cdot 19}$, а 1728 кратно 36.

Задачи для самостоятельного решения

Задача 6.6. Докажите, что каждое нечётное число n представимо как разность квадратов соседних натуральных чисел, а каждое нечётное составное число n представимо как разность квадратов двух несоседних чисел, то есть как $(u+k)^2 - u^2$ при $k > 1$.

Задача 6.7. Докажите, что если n — псевдопростое число по основанию 2, то $M_n = 2^n - 1 > n$ — также псевдопростое по основанию 2.

Задача 6.8. Докажите, что: а) если число Мерсенна $M_p = 2^p - 1$ составное (при простом p), то оно псевдопростое

(по основанию 2); б) если число Ферма $F_p = 2^{2^p} + 1$ составное (при простом p), то оно псевдопростое.

Задача 6.9. Псевдопростые числа могут быть чётными. Докажите, что $161038 = 2 \cdot 73 \cdot 1103$ — псевдопростое число (по основанию 2).

Задача 6.10. Докажите, что если числа $6k + 1$, $12k + 1$ и $18k + 1$ простые, то их произведение — число Кармайкла.

Задача 6.11. Докажите, что числами Кармайкла являются: а) $1105 = 5 \cdot 13 \cdot 17$; б) $6601 = 7 \cdot 23 \cdot 41$.

Задача 6.12. Найдите два различных числа Кармайкла вида $n = 13 \cdot 61 \cdot p$, где p — простое число.

Задача 6.13. Докажите, что никакое число Кармайкла не делится на квадрат какого-либо простого числа.

Решения и указания

6.6. Равенство $(u + 1)^2 - u^2 = 2u + 1$ даёт требуемое представление для произвольного нечётного числа $2u + 1$. Пусть теперь n — нечетное составное, а k — его наименьший делитель. Тогда n/k — другой (также нечётный, как и k) делитель n, причем n/k больше k на некоторое чётное число $2u$. Это означает, что $n = k(k + 2u) = (u + k)^2 - u^2$.

6.7. По условию, $n = rs$, где $1 < r \leqslant s < n$. Тогда $2^n - 1$ делится на $2^r - 1$, то есть M_n — составное. С другой стороны, $2^n \equiv 2 \pmod{n}$, то есть $2^n - 2 = kn$ для некоторого k. Отсюда $2^{M_n - 1} - 1 = 2^{kn} - 1$ делится на $2^n - 1 = M_n$, и, умножив на 2, получаем $2^{M_n} \equiv 2 \pmod{M_n}$. Это и доказывает псевдопростоту числа M_n.

6.8. а) Аналогично решению задачи 6.7.

б) Мы уже использовали в задаче 6.7, что число $2^b - 1$ делится на $2^a - 1$, если b делится на a. Поскольку большая степень двойки всегда делится на меньшую, то $2^{F_p - 1} - 1$ делится на $2^{2^{p+1}} - 1 = (2^{2^p} + 1)(2^{2^p} - 1)$, то есть делится на F_p. Отсюда $2^{F_p} - 2$ делится на F_p, а так как по условию F_p составное, то оно псевдопростое.

6.9. Заметим, что $2^9 \equiv 1 \pmod{73}$ и $2^{29} \equiv 1 \pmod{1103}$. Поскольку 161037 делится на 9 и на 29, имеем $2^{161037} \equiv \equiv 1 \pmod{161038}$, что и доказывает псевдопростоту числа.

6.10. В силу теоремы Корсельта достаточно доказать, что выражение $M = (6k+1)(12k+1)(18k+1) - 1$ делится на $6k$, $12k$ и $18k$. После раскрытия скобок получаем, что

$$M = (6\cdot 12\cdot 18)k^3 + (6\cdot 12 + 6\cdot 18 + 12\cdot 18)k^2 + (6+12+18)k.$$

Поэтому оно кратно $36k$, а следовательно, делится на $6k$, $12k$ и $18k$.

6.11. Снова воспользуемся теоремой Корсельта. В силу неё достаточно убедиться, что а) 1104 делится на 4, 12 и 16 (это так, поскольку $1104 = 2^4 \cdot 3 \cdot 23$), б) что 6600 делится на 6, 22 и 40 (все три утверждения очевидны).

6.12. По теореме Корсельта число $n - 1$ должно быть кратно 12, 60 и $p - 1$. То есть $13 \cdot 61 \cdot p \equiv 1 \pmod{60}$ и $13 \cdot 61 \cdot p \equiv 1 \pmod{p-1}$. Решая эти сравнения, получаем $p \equiv 37 \pmod{60}$ и $p - 1$ — делитель $13 \cdot 61 - 1 = 792$. Этим условиям удовлетворяют $p_1 = 37$ и $p_2 = 397$.

6.13. Предположим противное: $a^n \equiv a \pmod{n}$ для любого натурального a, и n делится на некоторое k^2. Для $a = k$ это означает $k^n \equiv k \pmod{n}$. Но так как n делится на k^2, это же сравнение выполнено по модулю k^2: $k \equiv k^n \equiv 0 \pmod{k^2}$. Но отсюда вытекает, что k делится на k^2, что, очевидно, невозможно.

Занятие 7

Шифрование с открытым ключом

Наука о шифровании — криптография — в течение многих веков служила людям для передачи секретных сообщений. Были придуманы десятки разных шифров, с помощью которых отправитель, знающий способ шифровки, мог закодировать свое сообщение, а получатель, знающий способ дешифровки, мог это сообщение раскодировать и прочитать. Как правило, все эти способы основывались на понятии «секретного» (или закрытого) ключа, т. е. опирались на сведения, известные только отправителю и получателю, но не постороннему человеку. Стойкость шифров определялась тем, какое время могло понадобиться постороннему для его вскрытия, то есть для того, чтобы суметь раскодировать и прочитать сообщение, не зная поначалу секретного ключа. Во все времена случались проколы, в результате которых секреты оказывались раскрытыми, а обладание секретами противника давало ощутимый перевес и в военных действиях, и в мирной дипломатии.

Опишем один из способов асимметричного шифрования, основанный на теории чисел. Пусть p — простое число, а e — число, взаимно простое с $p-1$. Если P — «исходное сообщение» — натуральное число, меньшее p, то ему можно сопоставить «шифрованное сообщение» — число C, равное остатку от деления P^e на p: $C \equiv P^e \pmod{p}$, $0 < C < p$. Таким образом, для шифрования нужно знать только два числа — p и e.

Теперь разберёмся с дешифрованием. По алгоритму Евклида, существует число $d < p$, для которого

$$de \equiv 1 \pmod{p-1}.$$

Вычислим C^d по модулю p: $C^d \equiv P^{ed} \equiv P \pmod{p}$ (в последнем сравнении использована МТФ). Таким образом, дешифрование сообщения C состоит в вычислении остатка



Рональд Ривест (р. 1947), Ади Шамир (р. 1952), Леонард Макс Адлеман (р. 1945) — современные специалисты по информатике, авторы одной из первых криптосистем с открытым ключом. Их совместная работа была опубликована в 1977 году. Как выяснилось позднее, все ключевые результаты их работы были открыты еще в 1973 году британским математиком Клиффордом Коксом, однако Кокс работал на GCHQ (Центр правительственной связи), поэтому результаты его исследований опубликованы не были.

от деления C^d на p. Тот, кто знает p и число d, сможет прочитать любое сообщение, закодированное этим шифром. Асимметричность шифрования здесь проявляется в том, что человек, знающий ключ шифрования, не сможет тем не менее расшифровать чужие сообщения, зашифрованные с этим же ключом, а человек, знающий ключ для дешифровки, не сможет ничего зашифровать. Впрочем, вычисление d по известным p и e (равно как и вычисление e по известным p и d) не является сложной задачей, так что надёжность такой системы невелика.

Однако во второй половине XX века появились действительно надёжные системы шифрования с публичным (открытым) ключом, то есть такие, для которых способ шифрования не нужно держать в секрете, — обладание общеизвестным ключом шифрования позволяет любому написать и зашифровать сообщение, но не позволяет расшифровать и прочитать сообщения, написанные другими. Эти системы также были основаны на некоторых фактах из теории чисел.

Метод RSA (названный по первым буквам фамилий авторов[1]) основан на следующем: Пусть $m = pq$ — составное число, равное произведению двух *больших*[2] простых чисел p и q. Зная эти числа, мы можем вычислить

$$\varphi(m) = (p-1)(q-1).$$

Выберем произвольное число e, взаимно простое с $\varphi(m)$. Открытым ключом является пара (m, e). Как и раньше, шифрование сообщения P состоит в вычислении остатка от деления P^e на m: $C \equiv P^e \pmod{m}$, $0 < C < m$. Однако знание открытого ключа не позволяет никому самостоятельно вычислить ни множители p и q, ни значение $\varphi(m)$. Мы же, зная $\varphi(m)$, можем вычислить такое d, для которого $de \equiv 1 \pmod{\varphi(m)}$, и с его помощью расшифровать полученное сообщение C: $P = C^d = P^{ed} \pmod{m}$ (здесь использована теорема Эйлера).

Еще раз поясним, почему этот способ считается надёжным. Ключ дешифрования состоит из чисел m и d. Число m известно (является частью открытого ключа), но число d держится в секрете. Если предположить, что злоумышленник вычислил d, то он будет знать

$$de - 1 \pmod{m} \equiv \varphi(m),$$

а так как $\varphi(m) = m - p - q + 1$, то это, в свою очередь, даст ему сумму $p + q$. Зная сумму двух простых чисел и их произведение, он сможет найти эти числа, то есть разложить число m на простые множители. Надёжность (стойкость)

[1]Большая часть работ XX века по криптографии до сих пор засекречена. Поэтому имена первооткрывателей алгоритмов криптографии не всегда известны. Это, разумеется, не умаляет заслуг тех учёных, которые переоткрыли их и сделали свои работы достоянием общественности.

[2]Слово «больших» здесь означает буквально следующее: если число m известно, должно быть затруднительно разложить его на множители за разумное время даже на самой мощной вычислительной технике. Поскольку это свойство, очевидно, зависит от мощности вычислительной техники, величина чисел, используемых для кодирования RSA, также от нее зависит. Тем не менее, так как убедиться в простоте числа проще, чем отыскать разложение составного числа на множители, фактически алгоритм RSA основан на том, что всегда будут существовать такие пары чисел, простоту которых мы проверить ещё можем, а вот найти разложение на множители их произведения, не зная заранее этих множителей, уже не можем.

системы RSA основана на том, что разложение большого составного числа на два (также больших) простых множителя требует очень значительных вычислительных ресурсов.

Задачи для самостоятельного решения

Задача 7.1. Найдите ключ дешифровки d для системы асимметричного шифрования, если известно, что $p = 2017$, $e = 13$.

Задача 7.2. Сгенерируйте ключи RSA по следующим исходным данным: $p = 3557$, $q = 2579$, $e = 3$.

Задача 7.3. Протокол Диффи—Хеллмана служит для того, чтобы создавать секретные ключи, пользуясь открытыми (общедоступными, незащищёнными, иначе говоря, ненадёжными) каналами связи. Пусть Алиса и Боб[1] знают два простых числа p и q. Эти числа[2] не секретны, они могут быть известны кому угодно. Чтобы создать общий и неизвестный более никому секретный ключ, Алиса сама генерирует большое случайное число a, а Боб — большое случайное число b. Затем Алиса вычисляет значение $A \equiv q^a \pmod{p}$ и пересылает его Бобу, а Боб вычисляет $B \equiv q^b \pmod{p}$ и пересылает Алисе. Числа A и B называются *открытыми ключами*, потому что предполагается, что пересылка происходит по открытому каналу связи, то есть злоумышленник может перехватить оба этих значения. Затем Алиса на основе имеющегося у неё закрытого ключа a и полученного открытого ключа B вычисляет значение $B^a \pmod{p}$, а Боб аналогично вычисляет $A^b \pmod{p}$. Докажите, что у Алисы и Боба получается одно и то же число. Объясните, почему это число действительно является секретным для всех остальных.

Задача 7.4. Придумайте, как расширить протокол Диффи—Хеллмана на трёх участников — Алису, Боба и Чарли.

---

[1] Традиционные имена персонажей криптографических протоколов. Впервые появились в работе Р. Ривеста в 1978 году.

[2] Для повышения надёжности число p выбирают очень большим и дополнительно требуют, чтобы $(p-1)/2$ также было простым числом. От числа q ничего такого не требуется, поэтому чаще всего используются простые числа первого десятка.

Задача 7.5. Придумайте, как использовать протокол Диффи—Хеллмана для шифрования с открытым ключом.

Решения и указания

7.1. Ответ: $d = 1861$.

Решение. Нужно решить сравнение $13d \equiv 1 \pmod{2016}$. Это можно сделать даже не раскладывая 2016 на множители — с помощью алгоритма Евклида для пары чисел (2016, 13). Собственно, поскольку $2016 = 13 \cdot 155 + 1$, имеем $13 \cdot 155 \equiv -1 \pmod{2016}$ и, следовательно,

$$13 \cdot (2016 - 155) \equiv 1 \pmod{2016}.$$

7.2. Ответ:

$$m = pq = 9173503, \quad \varphi(m) = (p-1)(q-1) = 9167368,$$
$$d \equiv 1/e \pmod{\varphi(m)} = 6111579$$

(последнее вычисление делается с помощью алгоритма Евклида).

7.3. Полученное число — это $K \equiv q^{ab} \pmod{p}$. Злоумышленник при этом знает, что оно является какой-то степенью известного ему числа A по известному модулю p и какой-то другой степенью известного ему числа B по модулю p, однако такие степени в результате могут давать любые остатки.

Комментарий. Задача вычисления ключа K по известным A и B называется задачей дискретного логарифмирования и считается трудноразрешимой. В статье Википедии «Discrete logarithm records» приведены текущие достижения в решении этой задачи.

7.4. Указание. В итоге у всех должен оказаться ключ, равный $q^{abc} \pmod{p}$. При этом злоумышленник может перехватить пересылавшиеся в открытом виде q^a, q^b, q^c, q^{ab}, q^{ac}, $q^{bc} \pmod{p}$, но это не даст ему никакого знания об общем секретном ключе.

7.5. Алиса публикует пару (p,q) в качестве своего открытого ключа. Боб выполняет свою часть вычислений и отсылает Алисе зашифрованное сообщение вместе с открытым ключом B.

Практические задачи

А. Вечный календарь

Обозначим число в месяце буквой q, а день недели буквой h. Пронумеруем дни числами от 0 (суббота) до 6 (пятница). Месяцы обозначим m и пронумеруем от 3 (март) до 14 (февраль), причем *будем относить январь и февраль к предыдущему году*. Номер года (обозначим его Y) разделим на 100 с остатком: $Y = 100J + K$.

Задача А1. Докажите, что для вычисления дня недели в григорианском календаре можно использовать *сравнение Зеллера*:

$$h \equiv q + \lfloor 13(m+1)/5 \rfloor + K + \lfloor K/4 \rfloor + \lfloor J/4 \rfloor - 2J \pmod 7.$$

Задача А2. Докажите, что в юлианском календаре[1] аналогичное сравнение имеет вид

$$h \equiv q + \lfloor 13(m+1)/5 \rfloor + K + \lfloor K/4 \rfloor + 5 - J \pmod 7.$$

Задача А3. Докажите, что перейти от h к более привычной нумерации дней недели (1 = понедельник, ..., 7 = воскресенье) можно по формуле $d = ((h+5) \bmod 7) + 1$.

Б. Метод Полларда для разложения на множители

Пусть n — (большое) составное число, а p — его наименьший простой делитель. Мы хотели бы выбрать числа $x_0, x_1, \ldots, x_s$ так, чтобы все они были различными по модулю n, но какие-то два из них (x_i и x_j) давали одинаковые остатки по модулю p. Если мы найдём эти два числа, то НОД$(x_i - x_j, n)$ будет нетривиальным делителем числа n,

[1] Юлианский календарь («старый стиль») отличается от григорианского («нового стиля») тем, что все годы, номера которых заканчиваются на 00, являются високосными. В григорианском календаре из годов, номера которых заканчиваются на 00, високосным является только каждый четвёртый. В частности, 2000 год был високосным, а 2100, 2200 и 2300 — не будут. Сейчас юлианский календарь отстает от григорианского на 13 дней.

а знание такого делителя позволит нам отыскать p. Число НОД$(x_i - x_j, n)$ может быть быстро найдено с помощью алгоритма Евклида. Проблема, однако, в том, что мы можем знать набор $x_0, x_1, \ldots, x_s$, но не знать, у какой именно пары совпали остатки по модулю p. А если проверять все пары чисел, придется сделать большое количество (порядка s^2) вычислений НОД. Дж. М. Поллард в 1974 году предложил удобный и эффективный способ уменьшить это количество.

Поллард строит больший набор (из $2m$ чисел), зато находит в нем нужную пару всего за m проверок, последовательно, по мере построения, проверяя лишь пары (x_m, x_{2m}). Набор он строит так: стартовав со случайного остатка x_0 по модулю n, он затем вычисляет $x_{k+1} = f(x_k) \pmod{n}$, $k = 1, 2, 3, \ldots$ для многочлена $f(x) = x^2 + 1$ (на самом деле можно использовать и другие многочлены степени выше 1). Но почему в такой последовательности обязательно подойдет какая-то из указанных пар?

Суть в том, что если d — делитель числа n (например, $d = p$), то $x_{k+1} \equiv f(x_k) \pmod{d}$ (это верно, даже если мы не знаем d). Но тогда рекуррентное задание чисел x_k гарантирует, что если $x_i \equiv x_j \pmod{d}$, то $x_{i+1} \equiv f(x_i) \equiv f(x_j) \equiv \equiv x_{j+1} \pmod{d}$. Иначе говоря, если в построенной последовательности нашлись два одинаковых остатка по модулю d, то дальше последовательность оказывается периодической по модулю d с периодом, делящим $j - i$. Длина периода не может быть больше, чем номер j первого из повторившихся элементов. Но тогда, если $s \geqslant j$ и s кратно длине периода, то $x_s \equiv x_{2s} \pmod{d}$.

Если же такая пара будет найдена до того, как последовательность зациклится по модулю n, то нужный нетривиальный делитель n будет найден.

Задача Б1. Для $n = 8051$, $x_0 = 2$, $f(x) = x^2 + 1$ вычислите все члены до x_6 включительно и докажите, что 97 — простой делитель числа 8051.

Задача Б2. Используйте метод Полларда для разложения на множители числа 533, используя следующие исходные данные:

А) $x_0 = 2$, $f(x) = x^2 + 1$;

Б) $x_0 = 3$, $f(x) = x^2 + 1$;
В) $x_0 = 2$, $f(x) = x^2 - 1$;
Г) $x_0 = 2$, $f(x) = x^3 + x + 1$.

Задача Б3. Разложите на множители $2^{58} + 1$ с помощью метода Полларда.

В. Организация турниров по круговой системе

Во многих игровых видах спорта (например, в шахматах и футболе) одна игра — это соревнование между двумя участниками, поэтому естественно возникает задача организации турниров для многих участников по круговой системе, то есть таких, чтобы в результате проведения нескольких последовательных туров каждый игрок (или команда) сыграл с каждым из остальных ровно один раз и при этом в турах не было большого числа свободных от игры участников.

Разумеется, если общее число участников нечётно, то в каждом туре хотя бы один из них вынужден отдыхать. Проще всего обеспечить это следующим способом: добавим одного «виртуального» участника, после чего общее количество участников станет чётным, а свободным от игры в каждом туре объявим того, кто в этом туре должен играть против виртуального участника.

Таким образом, достаточно разобраться со случаем чётного числа участников (команд). Перенумеруем их числами от 1 до N и составим расписание игр по следующей схеме: команды с номерами i, j, отличными от N, играют между собой в туре с номером $(i + j) \bmod (N - 1)$. Далее, существует ровно одна команда, номер которой удовлетворяет условию $2i \equiv k \pmod{N - 1}$. Именно эту команду в k-м туре назначим играть против команды N.

Задача В1. Докажите, что если туры 1, 2, ..., $N - 1$ устроены описанным выше образом, то каждая команда играет с каждой из остальных ровно один раз.

Задача В2. Постройте расписание кругового турнира для 5 команд.

Задача В3. Пусть, кроме расписания игр, мы должны выбрать, какой из игроков проводит игру «дома», а какой «на выезде». Сделаем это следующим образом: если $i + j$ нечётно, то «дома» играет игрок с меньшим номером, а если $i + j$ чётно — то с большим. Докажите, что при чётном числе туров (то есть при нечётном n) такое расписание обеспечивает, что каждый игрок проводит «дома» и «на выезде» поровну игр.

Г. Контрольные цифры

Задача Г1. Международный стандарт книжной нумерации (ISBN-10) задаёт 10-значный код для каждой книги, в котором 10-й знак вычисляется по правилу $a_{10} = a_1 + 2a_2 + ... + 9a_9 \pmod{11}$. (Если результат оказывается равным 10, то вместо цифры на месте a_{10} пишут букву X.)

а) При печати ISBN-10 две соседних цифры были переставлены. Докажите, что полученный таким образом код будет некорректным.

б) При печати ISBN-10 в одной из цифр была допущена ошибка. Докажите, что полученный код также будет некорректным.

Задача Г2. Международный стандарт нумерации музыкальных произведений (ISMN) задаёт 13-значный код, в котором 13-й знак вычисляется так, чтобы контрольная сумма

$$a_1 + 3a_2 + a_3 + 3a_4 + ... + a_{11} + 3a_{12} + a_{13}$$

делилась на 10. Аналогичным образом, только с 11 знаками вместо 13, устроен Universal Product Code — всем нам хорошо известный штрих-код на товарах. Докажите, что оба этих кода не обладают ни одним из свойств ISBN, доказанных в задаче Г1, пункты б) и в).

Задача Г3. Номер лицевого счёта для собственников квартир в Санкт-Петербурге — 9-значное число, в котором контрольная цифра стоит на последнем месте и определяется по следующему алгоритму: каждая цифра умножается на 2 в степени номера позиции (начиная с конца). Остаток

от деления на 11 суммы произведений затем вычитается из 11. Если результат больше 9, то результат принимается равным 0. Например, для номера 12345678 контрольная цифра равна 8: $11 - ((8 \cdot 2^1 + 7 \cdot 2^2 + 6 \cdot 2^3 + 5 \cdot 2^4 + 4 \cdot 2^5 + 3 \cdot 2^6 + 2 \cdot 2^7 + 1 \cdot 2^8) \bmod 11) = 8$. Хорош ли этот алгоритм с точки зрения чувствительности к ошибкам?

Дополнительные задачи

Задача Д1. Пусть $m = 2s + 1$ — нечётное натуральное число. Докажите, что множество $\{-s, 1 - s, ..., -1, 0, 1, ..., s - 1, s\}$ — полная система остатков по модулю m.

Задача Д2. Докажите, что $\{0, 1, 2, 2^2, ..., 2^9\}$ — полная система остатков по модулю 11.

Задача Д3. С помощью утверждения задачи 1.10 докажите признаки делимости а) на 9; б) на 11.

Задача Д4. Пусть x, y, z — целые числа, удовлетворяющие уравнению $x^2 + y^2 = z^2$. Докажите, что $xyz \equiv 0 \pmod{60}$.

Задача Д5. Найдите остатки от деления 100^{2015} а) на 99; б) на 101; в) на 9999.

Задача Д6. Найдите остаток от деления

$$2011 \cdot 2012 \cdot 2013 \cdot 2014 \cdot 2015$$

а) на 2010; б) на 2016.

Задача Д7. Докажите, что если $2^n - 1 \vdots 11$, то $2^n - 1 \vdots 93$.

Задача Д8. Докажите, что 2^{100} и 3^{100} сравнимы: а) по модулю 5; б) по модулю 13.

в) Найдите еще хотя бы один простой модуль, по которому эти числа также сравнимы.

Задача Д9. Докажите, что $(3^n - 1)^n - 4 \vdots 3^n - 4$ при любом натуральном n.

Задача Д10. Докажите, что $5^{2n} + 3 \cdot 2^{5n-2} \vdots 7$ при любом натуральном n.

Задача Д11. Докажите, что

а) $3^{n+2} + 4^{2n+1} \vdots 13$;

б) $6^{n+2} + 7^{2n+1} \vdots 43$;

в) $k^{n+2} + (k+1)^{2n+1} \vdots k^2 + k + 1$.

Задача Д12. Докажите, что $2^{5n+1} + 5^{n+2} \vdots 27$.

Задача Д13. Докажите, что если a — нечётное число, а n — натуральное, то $a^{2^n} \equiv 1 \pmod{2^{n+2}}$.

Задача Д14. Число a заканчивается на 33. На какие две цифры заканчивается a^{85}?

Задача Д15. Найдите три последних цифры числа 7^{2016}.

Задача Д16. Найдите все значения n, для которых $1! + 2! + \ldots + n!$ — полный квадрат.

Задача Д17. Пусть m — чётное число. Докажите, что если $\{a_1, a_2, \ldots, a_m\}$ и $\{b_1, b_2, \ldots, b_m\}$ — две полных системы остатков по модулю m, то $\{a_1 + b_1, a_2 + b_2, \ldots, a_m + b_m\}$ не является полной системой остатков по модулю m.

Задача Д18 (Московская олимпиада, 1969, 7 класс). Даны два целых положительных числа m и n. Известно, что сумма всех делителей m оказалась равна сумме всех делителей n и сумма чисел, обратных делителям n, оказалась равна сумме чисел, обратных делителям m. Докажите, что $m = n$.

* * *

Задача Д19. Докажите, что $(4n + 2)!! + (4n + 1)!! \vdots 4n + 3$ при любом натуральном n.

Задача Д20. Пусть $p \geqslant 5$ — простое число. Докажите, что $6(p - 4)! \equiv 1 \pmod{p}$.

Задача Д21. Вычислите остаток от деления $2000! \cdot 17!$ на 2017, если известно, что 2017 — простое число.

Задача Д22. Дано число 199!!. На какую наибольшую степень числа 3 оно делится?

* * *

Задача Д23. Докажите, что $n \vdots \varphi(n)$ только в следующих случаях: $n = 1$, $n = 2^k$, $n = 2^k 3^l$.

Задача Д24. Найдите все натуральные n, для которых $\varphi(5n) = 5\varphi(n)$.

Задача Д25. Пусть p и $2p - 1$ — нечётные простые числа. Докажите, что $\varphi(4p - 2) = \varphi(4p)$.

Задача Д26. Пусть $n = 5186$. Докажите, что

$$\varphi(n) = \varphi(n + 1) = \varphi(n + 2).$$

Задача Д27. Найдите все решения уравнения а) $\varphi(n) = 16$; б) $\varphi(n) = 24$.

Задача Д28. Докажите, что уравнение $\varphi(n) = 2p$ не имеет решений, если p простое, а $2p + 1$ — составное число.

Задача Д29. Выразите через $\varphi(n)$ сумму всех правильных несократимых дробей со знаменателем n.

Задача Д30. Докажите, что если $m \perp n$, то $m^{\varphi(n)} + n^{\varphi(m)} \equiv$ $\equiv 1 \pmod{mn}$.

Задача Д31. Докажите, что

$$\sum_{1 \leqslant i \leqslant n} \varphi(i) \left\lfloor \frac{n}{i} \right\rfloor = \frac{n(n+1)}{2}.$$

Задача Д32. Сколько существует таких натуральных k, для которых НОК$(k, 6^6, 8^8) = 12^{12}$?

Задача Д33. Найдите сумму всех натуральных чисел, меньших $2n$ и взаимно простых с n.

Задача Д34. Докажите, что если для некоторого натурального k существует единственное n такое, что $\varphi(n) = k$, то $n \vdots 36$.

Задача Д35 (Московская олимпиада, 1964, 10 класс). Имеется бесконечное количество карточек, на каждой из которых написано какое-то натуральное число. Известно, что для любого натурального числа n существует ровно n карточек, на которых написаны делители этого числа. Доказать, что каждое натуральное число встречается хотя бы на одной карточке.

Задача Д36. Сколько чисел, взаимно простых с 2015, встречается среди $1 \cdot 2, 2 \cdot 3, \ldots, 2015 \cdot 2016$?

* * *

Задача Д37. Докажите, что $3^{3000} - 1 \vdots 1001$.

Задача Д38. Докажите, что $n^7 - n \vdots 42$ при любом натуральном n.

Задача Д39. Докажите, что $n^{37} \equiv n \pmod{1729}$ при всех натуральных n. (Указание: $1729 = 7 \cdot 13 \cdot 19$.)

Задача Д40. Докажите, что $n^{15} - n^3$ делится на $2^{15} - 2^3$ при всех натуральных n.

Задача Д41. Математический хулиган Гриша катается на лифте 17-этажного дома. Он садится в лифт на этаже с номером n, меньшим 17, возводит номер этажа в квадрат и едет на этаж, номер которого равен остатку от деления результата на 17. После этого он возводит в квадрат номер этажа, на котором оказался, и едет на этаж с номером, равным остатку от деления на 17 полученного результата.

Если полученный номер совпадает с номером этажа, на котором Гриша уже находится, катание прекращается. Какое максимальное количество поездок ему удастся совершить таким способом?

Задача Д42. Найдите остаток от деления $2^{100\,000}$ на 31.

Задача Д43. а) Найдите показатель числа 10 по модулю 13. Найдите период десятичной дроби 1/13.

б) Докажите, что если $m \perp 10$, то длина периода дроби $1/m$ равна показателю 10 по модулю m.

Задача Д44. Назовём два многочлена с целыми коэффициентами эквивалентными по модулю m, если разность их значений в любой целой точке делится на m. Докажите, что каждый многочлен эквивалентен какому-то многочлену степени не выше $m - 1$.

Задача Д45. Пусть p и q — различные простые числа. Докажите, что

$$p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}.$$

Задача Д46. Последовательность (a_n) задана следующим образом: $a_0 = p$, где p — простое число, $a_{n+1} = 2a_n + 1$ для $n = 0, 1, 2, \ldots$ Докажите, что не существует такого p, для которого все члены этой последовательности являются простыми числами.

Задача Д47 (Международная математическая олимпиада, 2005). Рассмотрим последовательность

$$a_n = 2^n + 3^n + 6^n - 1.$$

Найдите все натуральные числа, взаимно простые с каждым членом этой последовательности.

Задача Д48. Докажите, что если $a \perp 10$, то последние три десятичные цифры чисел a и a^{2001} совпадают.

Задача Д49 (Китайский алгоритм). Пусть даны n попарно взаимно простых чисел $m_1, m_2, \ldots, m_n$ и n чисел $r_1, r_2, \ldots, r_n$, для которых $0 \leqslant r_i \leqslant m_i - 1$ при всех $i = 1, 2, \ldots, n$. Кроме того, пусть $M_i = M/m_i$, $i = 1, 2, \ldots, n$, где M — произведение всех m_i. Докажите, что число N, существование которого утверждается в КТО, может быть вычислено по формуле

$$N \equiv r_1 M_1^{\varphi(m_1)} + r_2 M_2^{\varphi(m_2)} + \ldots + r_n M_n^{\varphi(m_n)} \pmod{M}.$$

Решения и указания

Д1. Указание. Добавьте по $m = 2s + 1$ ко всем отрицательным элементам множества.

Д2. Указание. Достаточно доказать, что разность любых двух из 11 выбранных элементов не делится на 11.

Д3. а) Десятичную запись натурального числа

$$\overline{a_n a_{n-1} \ldots a_0} = a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \ldots + a_0 \cdot 10^0$$

можно рассматривать как значение многочлена с целыми коэффициентами в точке $a = 10$. При этом сумма цифр числа — это значение того же многочлена в точке $b = 1$. Так как $10 \equiv 1 \pmod 9$, из задачи 1.10 получаем утверждение о том, что каждое число сравнимо со своей суммой цифр по модулю 9 — а это и есть обобщённый признак делимости на 9 (точнее говоря, это признак равноостаточности по модулю 9).

б) Знакочередующаяся сумма цифр

$$(-1)^n a_n + (-1)^{n-1} a_{n-1} + \ldots + a_0$$

— это значение этого же самого многочлена в точке $b = -1$. Так как $10 \equiv -1 \pmod{11}$, из задачи 1.10 получаем утверждение о том, что каждое число сравнимо со своей знакочередующейся суммой цифр по модулю 11.

Д4. Рассмотрите отдельно делимость xyz на 3, 4 и 5. Например, рассуждение по модулю 5 может быть таким: если ни x, ни y не делятся на 5, то их квадраты при делении на 5 дают остатки 1 или 4. Тогда $x^2 + y^2$ даёт остаток $1 + 1$, $1 + 4$ или $4 + 4$. Из трёх этих вариантов квадратом может быть только $1 + 4 \equiv 0 \pmod 5$, то есть z делится на 5, откуда сразу получаем, что xyz делится на 5.

Д5. а) $100 \equiv 1 \pmod{99}$, поэтому

$$100^{2015} \equiv 1^{2015} \equiv 1 \pmod{99}.$$

б) $100 \equiv -1 \pmod{101}$, поэтому

$$100^{2015} \equiv (-1)^{2015} \equiv -1 \pmod{101}.$$

в) $100^{2015} = (100^2)^{1007} \cdot 100^1 = 10000^{1007} \cdot 100 \equiv 1^{1007} \cdot 100 \equiv$
$\equiv 100 \pmod{9999}$.

Комментарий. Подумайте, как вывести в) из результатов а) и б). Обратите внимание на то, как использование отрицательного числа -1 в пункте б) избавило от выполнения умножений.

Д6. а) Заменим каждое число его остатком. По свойству произведения сравнений получим

$$2011 \cdot 2012 \cdot 2013 \cdot 2014 \cdot 2015 \equiv 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 = 120 \pmod{2010}.$$

Так как $0 \leqslant 120 < 2010$, оно и является остатком от деления произведения шести указанных чисел на 2010.

б) Здесь удобнее заменить каждое число сравнимым с ним отрицательным числом. Тогда по свойству произведения получим

$$2011 \cdot 2012 \cdot 2013 \cdot 2014 \cdot 2015 \equiv$$
$$\equiv (-5) \cdot (-4) \cdot (-3) \cdot (-2) \cdot (-1) = -120 \pmod{2016}.$$

Поэтому искомым остатком будет число $2016 - 120 = 1896$.

Д7. Здесь снова помогает рассмотрение циклов. По модулю 11:

$$2^0 = 1, \quad 2^1 = 2, \quad 2^2 = 4, \quad 2^3 = 8, \quad 2^4 = 16 \equiv 5,$$
$$2^5 \equiv 10, \quad 2^6 \equiv 10 \cdot 2 \equiv 9, \quad 2^7 \equiv 9 \cdot 2 \equiv 7, \quad 2^8 \equiv 7 \cdot 2 \equiv 3,$$
$$2^9 \equiv 3 \cdot 2 = 6, \quad 2^{10} \equiv 6 \cdot 2 \equiv 1.$$

Далее остатки повторяются, поэтому мы делаем вывод о делимости $2^n - 1$ на 11: $2^n - 1 \equiv 0 \pmod{11} \Leftrightarrow n \vdots 10$. Число 93 не простое, поэтому лучше рассмотреть его простые делители 3 и 31. По модулю 31: $2^0 = 1$, $2^1 = 2$, $2^2 = 4$, $2^3 = 8$, $2^4 = 16$, $2^5 = 32 \equiv 1$, и делается аналогичный вывод: $2^n - 1 \equiv 0 \pmod{31} \Leftrightarrow n \vdots 5$. По модулю 3 всё ещё проще: любая чётная степень двойки сравнима с 1. Так как любое число, делящееся на 10, делится на 5 и на 2, то утверждение задачи доказано.

Д8. а) Здесь тоже можно было бы поступить аналогично решению задач 1.6, 1.11, Д7 и сосчитать несколько первых остатков (до зацикливания), но мы покажем более простой способ. Из сравнения $3 \equiv -2 \pmod 5$ следует, что $3^{100} \equiv (-2)^{100} = (-1)^{100} 2^{100} \equiv 2^{100} \pmod 5$.

б) Аналогично, $3^2 = 9 = -4 = -2^2 \pmod{13}$. Отсюда $3^{100} = 9^{50} \equiv (-2^2)^{50} = 2^{100} \pmod{13}$.

в) Решение задач а) и б) наводит на идею поискать такое простое p, которое равно $3^d + 2^d$ для некоторого d, являющегося делителем числа 100. На первый взгляд, годится $d = 4$ и $p = 3^4 + 2^4 = 97$, однако тогда $3^{100} = (3^4)^{25} \equiv (-2^4)^{25} = -2^{100} \pmod{97}$, а не $2^{100} \pmod{97}$. В чем причина неудачи? Очевидно, мешает нечётность числа $100/4 = 25$. Пробуем следующий делитель $d = 5$, но число $3^5 + 2^5 = 275$ не простое. Зато оно содержит простой множитель 11, поэтому

$$3^{100} = (3^5)^{20} = (-2^5)^{20} = 2^{100} \pmod{11}.$$

Комментарий. Другой вариант — рассмотреть делимость на $p = 3^5 - 2^5 = 211$.

Д9. $3^n - 1 \equiv 3 \pmod{(3^n - 4)}$. Поэтому

$$(3^n - 1)^n - 4 \equiv 3^n - 4 \equiv 0 \pmod{(3^n - 4)}.$$

Д10. $5^{2n} + 3 \cdot 2^{5n-2} = 25^n + 3 \cdot 2^{5n-2} \equiv 32^n + 3 \cdot 2^{5n-2} = (4 + 3) \cdot 2^{5n-2} \equiv 0 \pmod{7}$.

Д11. а) Имеем

$$3^{n+2} + 4^{2n+1} = 9 \cdot 3^n + 4 \cdot 16^n \equiv (9 + 4) \cdot 3^n \equiv 0 \pmod{13}.$$

Пункт б), как и а), является частным случаем пункта в).

в) Имеем

$$k^{n+2} + (k+1)^{2n+1} = k^2 \cdot k^n + (k+1)(k^2 + 2k + 1)^n \equiv$$

$$\equiv k^2 \cdot k^n + (k+1)k^n = (k^2 + k + 1)k^n \equiv 0 \pmod{k^2 + k + 1}.$$

Д12. Указание. Воспользуйтесь тем, что $32 \equiv 5 \pmod{27}$ и $2 + 25 \equiv 0 \pmod{27}$.

Д13. Указание. Воспользуйтесь методом математической индукции. Базу индукции ($n = 1$) доказать нетрудно: $a - 1$ и $a + 1$ — два последовательных чётных числа, поэтому одно из них кратно 4, а значит, их произведение кратно 8.

Д14. Указание. Умножать число 33 на себя 85 раз — не лучшая идея, и искать цикл по модулю 100 тоже не нужно. Собственно, смысл этого упражнения как раз в том, чтобы придумать, как обойтись сравнительно небольшим числом умножений.

Решение 1. По условию $a \equiv 33 \pmod{100}$, тогда

$$a^2 = 33 \cdot 33 = 1089 \equiv -11 \pmod{100},$$
$$a^4 = (-11) \cdot (-11) \equiv 21 \pmod{100},$$
$$a^8 = a^4 \cdot a^4 \equiv 21 \cdot 21 \equiv 41 \pmod{100},$$
$$a^{16} = a^8 \cdot a^8 = 41 \cdot 41 \equiv 81 \pmod{100},$$
$$a^{17} = a \cdot a^{16} \equiv 33 \cdot 81 \equiv 73 \pmod{100},$$
$$a^{34} = a^{17} \cdot a^{17} \equiv 73 \cdot 73 \equiv 29 \pmod{100},$$
$$a^{68} \equiv 29 \cdot 29 \equiv 41 \pmod{100},$$
$$a^{85} = a^{68} \cdot a^{17} \equiv 41 \cdot 73 \equiv 93 \pmod{100}.$$

Комментарии. 1. Нам хватило всего 8 умножений, а цикл имеет длину 20, поэтому если бы мы досчитывали все степени подряд до появления цикла, то вычислительной работы было бы больше.

2. Набор промежуточных степеней у нас был таким: 2, 4, 8, 16, 17, 34, 68. Иначе говоря, мы сначала добрались до числа 17 — наибольшего простого делителя числа 85 — а затем два раза его удвоили (это соответствует возведению в квадрат). Можно было бы воспользоваться и другим простым делителем: найти остатки от a в степени 2, 4, 5, 10, 20, 40, 80, а затем использовать равенство $85 = 80 + 5$. Это дало бы результат за те же 8 умножений.

Решение 2. Будем последовательно возводить числа в квадрат, увеличивая найденную степень вдвое. Вплоть до a^{16} мы это уже сделали в решении 1, далее $a^{32} \equiv 81 \cdot 81 \equiv$ $\equiv 61 \pmod{100}$, $a^{64} \equiv 61 \cdot 61 \equiv 21 \pmod{100}$. Теперь осталось перемножить нужные степени a: $a^{85} = a \cdot a^4 \cdot a^{16} \cdot a^{64} \equiv$ $\equiv 33 \cdot 21 \cdot 81 \cdot 21 \equiv 93 \pmod{100}$.

Комментарий 3. Решение 2 требует 9 умножений, то есть менее экономно. Зато оно более универсально, так как позволяет вычислить результат для любой степени, не раскладывая ее на множители, а воспользовавшись двоичной записью. Впрочем, достаточно часто такой способ является одновременно и самым экономным. Последовательность A003313 перечисляет минимальное число умножений, тре-

буемых для возведения в n-ю степень, а A014701 — количество умножений, требуемых для возведения в степень «двоичным» методом (как в решении 2). Среди 50 первых значений этих двух последовательностей 40 значений совпадают, и только для 10 значений n «двоичный» метод хуже оптимального (на одно умножение).

Д15. $7^4 \equiv 401 \pmod{1000}$, поэтому $7^{4n} \equiv (1 + 400)^n \equiv \equiv 1 + 400n$. Так как $2016 = 4 \cdot 504$, а

$$1 + 400 \cdot 504 \equiv 601 \pmod{1000},$$

то 7^{2016} заканчивается на 601.

Д16. При $n = 1$ получаем полный квадрат, при $n = 2$ — нет, при $n = 3$ — опять полный квадрат, при $n = 4$ — нет. При $n \geqslant 5$

$$1! + 2! + 3! + 4! + \ldots + n! \equiv 1! + 2! + 3! + 4! \equiv 3 \pmod{10},$$

поэтому полным квадратом сумма быть не может.

Д17. Предположим противное. Тогда

$$\begin{aligned} 1 + 2 + \ldots + m &\equiv (a_1 + b_1) + (a_2 + b_2) + \ldots + (a_m + b_m) = \\ &= (a_1 + a_2 + \ldots + a_m) + (b_1 + b_2 + \ldots + b_m) \equiv \\ &\equiv 2(1 + 2 + \ldots + m) \pmod{m}. \end{aligned}$$

Отсюда получается, что $1 + 2 + \ldots + m \equiv 0 \pmod{m}$, то есть $m(m + 1)/2 \vdots m$, что невозможно при чётном m. Противоречие.

Д18. Если k — делитель n, то n/k — тоже делитель n. Если $d_1, d_2, \ldots, d_s$ — все делители числа n, а $e_1, e_2, \ldots, e_t$ — все делители числа m, то имеем

$$d_1 + d_2 + \ldots + d_s = n\left(\frac{1}{d_1} + \frac{1}{d_2} + \ldots + \frac{1}{d_s}\right)$$

и

$$e_1 + e_2 + \ldots + e_t = m\left(\frac{1}{e_1} + \frac{1}{e_2} + \ldots + \frac{1}{e_t}\right).$$

Приравнивая левые части и учитывая, что

$$\frac{1}{d_1} + \frac{1}{d_2} + \ldots + \frac{1}{d_s} = \frac{1}{e_1} + \frac{1}{e_2} + \ldots + \frac{1}{e_t}$$

(по условию), получаем $m = n$.

Д19. Число $(4n+2)!!$ содержит $2n+1$ множителей: $2, 4, 6, \ldots, 4n+2$. Первый из них сравним с $-(4n+1)$, второй с $-(4n-1)$, ..., последний с (-1) по модулю $4n+3$. По свойству произведения, $(4n+2)!! \equiv (-1)^{2n+1}(4n+1)!! = -(4n+1)!!$, откуда $(4n+2)!! + (4n+1)!! \equiv 0 \pmod{4n+3}$.

Д20. По теореме Вильсона $(p-1)! \equiv -1 \pmod{p}$. Перепишем это в виде $(p-4)!(p-3)(p-2)(p-1) \equiv -1 \pmod{p}$ и воспользуемся сравнениями $p-3 \equiv -3$, $p-2 \equiv -2$, $p-1 \equiv -1$. Получим $(p-4)!(-6) \equiv -1 \pmod{p}$, откуда $6(p-4)! \equiv 1 \pmod{p}$.

Д21. По модулю 2017 имеем $16! \equiv (-2016)(-2015) \cdot \ldots \cdot (-2001)$, поэтому $2000! \cdot 16! \equiv 2016! \equiv -1$. Отсюда

$$2000! \cdot 17! \equiv -17 \equiv 2000.$$

Д22. В произведение 199!! входят 33 числа, кратные трём: 3, 9, 15, 21, ..., 195. Таким образом, это произведение делится на 3^{33}. Если уменьшить втрое каждое из чисел, кратных 3, некоторые будут по-прежнему делиться на 3. Таких чисел останется 11 — это ровно те числа, которые изначально (до уменьшения) делились на 9 (то есть числа 9, 27, 45, ..., 189). Аналогично, после сокращения на 3^{11} останутся 4 числа (полученные из 27, 81, 135, 189), которые по-прежнему делятся на 3, и еще одно число (полученное из 81) можно будет сократить на 3 в четвёртый раз. Итого получается, что 199!! делится на $3^{33+11+4+1} = 3^{49}$.

Д23. Из формулы

$$\varphi(n) = n \prod_i \left(1 - \frac{1}{p_i}\right)$$

следует, что целое число $n/\varphi(n)$ должно быть равно произведению тех из дробей $2/1, 3/2, 5/4, 7/6, \ldots$, числители которых являются простыми делителями n. Так как в числителе произведения таких дробей содержится не более одной двойки, то в знаменателе может быть не более одного числа $p-1$, где p — нечётное простое. Следовательно, n имеет не более одного нечётного простого множителя. Следовательно, либо n — степень двойки (и тогда $\varphi(n) = n/2$, как следует из задачи 3.11), либо $n = 2^k p^l$, и тогда

$\varphi(n) = 2^{k-1}p^{l-1}(p-1)$, откуда $n/\varphi(n) = 2p/(p-1)$. Так как это число целое, то $p-1=2$, $p=3$, $n=2^k3^l$.

Д24. Ответ: все числа, кратные 5.

Решение. Для начала отметим, что НОД$(5, n) > 1$, т.к. иначе было бы $\varphi(5n) = \varphi(5)\varphi(n) = 4\varphi(n)$. Поэтому $n \vdots 5$. Пусть $n = 5m$. Получили уравнение $\varphi(25m) = 5\varphi(5m)$. Докажем, что его решением является произвольное натуральное число m. Действительно, если $m = 5^t m'$, где $m' \perp 5$, то $\varphi(25m) = \varphi(5^{t+2}m') = 4 \cdot 5^{t+1}\varphi(m')$ и $5\varphi(5m) = 5\varphi(5^{t+1}m') = 4 \cdot 5^{t+1}\varphi(m')$.

Комментарий. В условии этой задачи число 5 можно заменить на любое другое простое число.

Д25. Имеем

$$\varphi(4p) = \varphi(4)\varphi(p) = 2(p-1);$$
$$\varphi(4p-2) = \varphi(2)\varphi(2p-1) = 1(2p-2).$$

Д26. Имеем $n = 2 \cdot 2593$, где 2593 — простое, поэтому $\varphi(n) = 1 \cdot 2592$; $n+1 = 3 \cdot 7 \cdot 13 \cdot 19$, поэтому $\varphi(n+1) = 2 \cdot 6 \cdot 12 \cdot 18 = 2592$. И, наконец, $n+2 = 2 \cdot 2 \cdot 1297$, где 1297 — простое, поэтому $\varphi(n+2) = 2 \cdot 1296 = 2592$.

Комментарий. Равенство $\varphi(5186) = \varphi(5188)$ следует из результата задачи Д25 для $p = 1297$.

Д27. а) В силу мультипликативности (задача 3.4) $\varphi(n)$ равно произведению чисел $\varphi(p^k)$, где p^k — максимальная степень простого числа p, делящая n. Следовательно, такие значения могут быть равны 1 (для $p^k = 2$), 2 (для $p^k = 3$ или 2^2), 4 (для $p^k = 5$ или 2^3), 8 (для $p^k = 2^4$) или 16 (для $p^k = 17$ или 2^5). Выбрав (шестью возможными способами), на какую наибольшую степень двойки делится n, мы затем уже однозначно сможем определить нечётные простые делители. Итак, возможны варианты $n = 17, 32, 34, 40, 48, 60$.

б) Аналогично, выпишем возможные варианты для отдельных взаимно простых множителей: 1 (для $p^k = 2$), 2 (для $p^k = 3$ или 2^2), 4 (для $p^k = 5$ или 2^3), 6 (для $p^k = 7$ или 3^2), 8 (для $p^k = 2^4$) или 12 (для $p^k = 13$). Соответственно, разложение $24 = 4 \cdot 6$ даёт варианты $n = 5 \cdot 7, 5 \cdot 9, 8 \cdot 7, 8 \cdot 9$, разложение $24 = 2 \cdot 12$ даёт варианты $n = 3 \cdot 13$ и $4 \cdot 13$, а разложение $24 = 1 \cdot 2 \cdot 12$ добавляет ещё вариант $n = 2 \cdot 3 \cdot 13$.

И наконец, разложение $24 = 2 \cdot 2 \cdot 6$ даёт вариант $n = 3 \cdot 4 \cdot 7$, разложение $24 = 1 \cdot 4 \cdot 6$ даёт два варианта $n = 2 \cdot 5 \cdot 7$ и $2 \cdot 5 \cdot 9$, а разложение $24 = 1 \cdot 2 \cdot 2 \cdot 6$ даёт ещё один вариант $n = 2 \cdot 3 \cdot 4 \cdot 7$.

Д28. Пусть q — простой делитель числа n. Так как $q - 1$ должно быть делителем числа $\varphi(n) = 2p$, возможны варианты $q - 1 = 1, 2, p, 2p$. Но последний вариант невозможен из-за того, что $2p + 1$ — составное число, а вариант $q - 1 = p$ означает, что оба числа q и $q - 1$ простые, но это возможно только при $q - 1 = 2$. Таким образом, осталось рассмотреть только $q = 2$ и $q = 3$. Иначе говоря, простыми делителями n могут быть только 2 и 3, откуда $n = 2^a 3^b$. Если a и b положительны, то $\varphi(n) = 2^a 3^{b-1}$, откуда $p = 2^{a-1} 3^{b-1}$, то есть возможно только $p = 2$ и $p = 3$. Но числа $2 \cdot 2 + 1$ и $2 \cdot 3 + 1$ не составные — противоречие. Если $n = 2^a$, то $\varphi(n) = 2^{a-1}$, откуда $a = 3$, т. е. опять же $p = 2$, что невозможно. Если, наконец, $n = 3^b$, то получаем невозможное равенство $p = 3$.

Д29. Пусть $n > 2$. Если $a \perp n$, то и $(n - a) \perp n$, поэтому обе дроби a/n и $(n - a)/n$ несократимы одновременно. Их сумма равна 1, и они различны, иначе обе равны $1/2$ и $n = 2$. Количество чисел, взаимно простых с n, равно $\varphi(n)$, поэтому сумма несократимых дробей будет равна $\varphi(n)/2$. При $n = 2$ сумма дробей состоит из одного слагаемого $1/2$ и, следовательно, тоже равна $\varphi(2)/2$.

Д30. По теореме Эйлера $m^{\varphi(n)} + n^{\varphi(m)} \equiv 0 + 1 \pmod{m}$ и $m^{\varphi(n)} + n^{\varphi(m)} \equiv 1 + 0 \pmod{n}$. Следовательно, $m^{\varphi(n)} + n^{\varphi(m)} - 1$ делится и на m, и на n, а значит, делится на $\text{НОК}(m, n) = mn$.

Д31. Воспользуемся тождеством Гаусса

$$k = \sum_{k:d} \varphi(d)$$

и просуммируем обе части этого равенства по всем k от 1 до n. Ясно, что при этом будут просуммированы числа $\varphi(d)$ при всех $d \leqslant n$, причем многие — по нескольку раз. Главный вопрос — сколько раз будет просуммировано слагаемое $\varphi(d)$ для каждого возможного d? Очевидно, что $\varphi(d)$ входит в сумму для тех и только тех индексов k, которые делятся на d, то есть для чисел $d, 2d, 3d, \ldots, [n/d]d$. Значит, слагаемое $\varphi(d)$ входит в итоговую сумму ровно $[n/d]$ раз,

что и указано в левой части доказываемого равенства. Ну а правая часть $n(n+1)/2$, как известно, равна сумме $1+2+\ldots+n$.

Д32. Ответ: 25.

Решение. Выпишем канонические разложения:

$$6^6 = 2^6 \cdot 3^6, \quad 8^8 = 2^{24}, \quad 12^{12} = 2^{24} \cdot 3^{12}.$$

Так как ни 6^6, ни 8^8 не делятся на 3^{12}, число k обязано делиться на 3^{12} (но не на большую степень тройки). Кроме того, оно может делиться на степени 2, не превосходящие 24, но не может делиться ни на какие иные простые числа. Таким образом, в качестве искомых k годятся только числа вида $2^n \cdot 3^{12}$, $n = 0, 1, \ldots, 24$, — всего 25 чисел.

Д33. Ответ: $2n\varphi(n)$.

Д34. Указание. Для каждого из случаев «n нечётно», «n делится на 2, но не делится на 4», «n не кратно 3», «n кратно 3, но не кратно 9» можно предъявить два различных значения n с одинаковыми значениями $\varphi(n)$.

Д35. Указание. Пусть $k(n)$ — число карточек, на которых написано число n. Тогда по условию $n = \sum\limits_{n \vdots d} k(d)$ для каждого n. Методом математической индукции будем доказывать, что $k(n) = \varphi(n)$ для всех n. Если для всех $m < n$ равенство $k(m) = \varphi(m)$ уже доказано, то из тождества Гаусса (совпадения полных сумм) сразу вытекает, что $k(n) = \varphi(n)$. А так как $\varphi(n) > 0$, каждое число написано хотя бы на одной карточке.

Д36. Указание. Разложение 2015 на множители имеет вид $2015 = 5 \cdot 13 \cdot 31$. Функция «количество чисел вида $k(k+1)$, взаимно простых с N» мультипликативна и равна $p-2$ на простых числах p. Поэтому для 2015 она равна $3 \cdot 11 \cdot 29 = 957$.

Д37. $1001 = 7 \cdot 11 \cdot 13$. Аналогично задаче 5.12, применить МТФ отдельно для модуля 7 ($n = 3^{500}$, $n^6 \equiv 1$), модуля 11 ($n = 3^{300}$, $n^{10} \equiv 1$) и модуля 13 ($n = 3^{250}$, $n^{12} \equiv 1$).

Д38. Аналогично задачам 5.12 и Д37, отдельно рассмотрим сравнения по модулям 7, 3 и 2. Если n делится на какой-то из модулей, то и $n(n^6-1)$ делится на него, а если

n не делится на модуль из множества $\{2, 3, 7\}$, то $n^6 - 1$ делится на него по МТФ.

Д39. $n^{37} - n$ делится на n, $n^6 - 1$, $n^{12} - 1$ и на $n^{18} - 1$. Пара делителей $(n, n^{p-1} - 1)$ гарантирует делимость выражения на p при всех n, и это можно применить для каждого p из множества $\{7, 13, 19\}$.

Д40. $2^{15} - 2^3 = 2^3(2^6 - 1)(2^6 + 1) = 2^3 \cdot 3^2 \cdot 5 \cdot 7 \cdot 13$. Докажем делимость отдельно на каждый из простых множителей. Для этого заметим, что $\varphi(13) = 12$, $\varphi(9) = \varphi(7) = 6$, $\varphi(8) = \varphi(5) = 4$. Поэтому $n^{12} - 1$ делится на $5, 7, 8, 9, 13$, если n взаимно просто с данным делителем. Если же n делится на один из простых делителей числа $2^{15} - 2^3$, то n^3 и n^{15} делятся на его куб.

Д41. Гриша последовательно побывает на этажах

$$n,\ n^2 \pmod{17},\ n^4 \pmod{17},\ n^8 \pmod{17},\ n^{16} \pmod{17}.$$

Последний из этих этажей по МТФ сравним с 1 для любого n, то есть будет первым этажом. При дальнейшем возведении в квадрат он останется равен 1, то есть больше лифт никуда не поедет. Таким образом, мы доказали, что максимально возможное число поездок не превосходит 4. Четыре поездки возможны, например, при $n = 3$: сначала Гриша приедет на 9 этаж, потом на $9^2 \pmod{17} \equiv 13$, потом на $13^2 \pmod{17} \equiv 16$ и, наконец на $16^2 \pmod{17} \equiv 1$.

Д42. $2^5 \equiv 1 \pmod{31}$, поэтому $2^{100\,000} \equiv 1 \pmod{31}$.

Д43. а) Как уже отмечалось в задаче Д37,

$$1001 = 10^3 + 1 \vdots 13,$$

поэтому $10^6 - 1 \equiv 0 \pmod{13}$. Также нетрудно убедиться, что $10^1, 10^2, \ldots, 10^5$ не равны 1 по модулю 13, поэтому показатель 10 по модулю 13 равен 6.

Чтобы найти период десятичной дроби $1/13$, начнем делить 1 на 13 в столбик: $1/13 = 0{,}076923\ldots$ Процесс деления продолжим до тех пор, пока остаток в какой-то момент не станет равным 1. Начиная с этого момента цифры в частном начнут повторяться, то есть мы нашли искомый период: $1/13 = 0{,}(076923)$.

б) Аналогично пункту а), если $m \perp 10$, то рано или поздно среди получаемых при делении 1 на m в столбик остатков вновь встретится 1. Если это впервые произошло на l-м шаге, то $10^l - 1 = mq$, что и означает, что l — показатель 10 по модулю m.

Д44. Достаточно убедиться в том, что каждый из многочленов x^m, x^{m+1}, x^{m+2}, ... эквивалентен иксу в меньшей степени. Это следует из того, что $x^{1+\varphi(m)}$ эквивалентен x^1.

Д45. $p^{q-1} \equiv 1 \pmod q$ и $q^{p-1} \equiv 1 \pmod p$ в силу МТФ. Следовательно, $p^{q-1} + q^{p-1}$ сравнимо с 1 и по модулю p, и по модулю q. А значит, $p^{q-1} + q^{p-1} - 1$ делится на произведение pq.

Д46. Нетрудно проверить формулу общего члена последовательности: $a_n = 2^n p + (2^n - 1)$. Это означает, что $a_n \equiv 2^n - 1 \pmod p$. Без ограничения общности можно считать, что p нечётно (если $p = 2$, то $a_1 = 5$, так что можно начать последовательность со следующего члена). Но по МТФ получается, что $a_{p+1} \equiv 0 \pmod p$. Поскольку $a_{p+1} > p$, число a_{p+1} составное.

Д47. Ответ: 1.

Решение. Достаточно доказать, что для каждого простого p существует член последовательности, кратный p. Для $p = 2$ и $p = 3$ таковым является $a_2 = 48$. Пусть теперь $p \geqslant 5$. По МТФ $2^{p-1} \equiv 3^{p-1} \equiv 6^{p-1} \equiv 1 \pmod p$, откуда $3 \cdot 2^{p-1} + 2 \cdot 3^{p-1} + 6^{p-1} \equiv 6 \pmod p$, или $6(a_{p-2} + 1) \equiv 6 \pmod p$. Поэтому $a_{p-2} \equiv 0 \pmod p$, что и требовалось доказать.

Д48. $\varphi(1000) = 400$, поэтому $a^{400} \equiv 1 \pmod{1000}$, а так как $2001 \equiv 1 \pmod{1000}$, получаем $a^{2001} \equiv a \pmod{1000}$, что и означает совпадение трёх последних цифр.

Д49. Каждый множитель $M_i^{\varphi(m_i)}$ по теореме Эйлера даёт остаток 1 при делении на m_i и остаток 0 при делении на все остальные модули. Поэтому слагаемое $r_i M_i^{\varphi(m_i)}$ даёт остаток r_i при делении на m_i и остаток 0 по всем остальным модулям. Следовательно, вся сумма даёт нужные остатки по всем модулям.

Раздаточный материал

Занятие 1. Арифметика остатков

Задача 1.1. Докажите, что если $a \equiv b \pmod m$ и $c \equiv d \pmod m$, то
а) $a + c \equiv b + d \pmod m$;
б) $ac \equiv bd \pmod m$.

Задача 1.2. Докажите, что если $a \equiv b \pmod m$ и k — натуральное число, то $a^k \equiv b^k \pmod m$.

Задача 1.3. Пусть m — натуральное число. Докажите, что множество $\mathrm{M} = \{0, 3, 6, \ldots, 3m - 3\}$ образует полную систему остатков тогда и только тогда, когда $m \perp 3$.

Задача 1.4. Постройте таблицу умножения по модулю 5.

Задача 1.5. Постройте таблицу умножения по модулю 6.

Задача 1.6. Найдите наименьшие неотрицательные остатки для $6^k + 1 \pmod{17}$ при $k = 1, 2, 3, 4, 5$.

Задача 1.7. а) Пусть m — нечётное натуральное число. Докажите, что множество $\{0, 2, 4, \ldots, 2m - 2\}$ — полная система остатков по модулю m. б) Пусть $k \perp m$. Докажите, что множество $\{0, k, 2k, \ldots, (m - 1)k\}$ — полная система остатков по модулю m. в) Пусть $k \perp m$, r — произвольное число. Докажите, что $\{r, k + r, 2k + r, \ldots, (m - 1)k + r\}$ — полная система остатков по модулю m.

Задача 1.8. Пусть $d \perp m$ и $ad \equiv bd \pmod m$. Тогда $a \equiv b \pmod m$.

Задача 1.9. Пусть d — натуральное число, являющееся общим делителем a, b и m. Докажите, что сравнения $a \equiv b \pmod m$ и $a/d \equiv b/d \pmod{m/d}$ равносильны.

Задача 1.10. Пусть $p(x)$ — многочлен с целыми коэффициентами и $a \equiv b \pmod m$. Тогда $p(a) \equiv p(b) \pmod m$.

Задача 1.11. Докажите, что $7^{2014} + 9^{2014} \vdots 10$.

Задача 1.12. Докажите, что ни при каком натуральном n число $3^n + 5^n$ не является полным квадратом.

Задача 1.13. Последовательность (a_n) задана формулами $a_1 = a_2 = 1$, $a_{n+2} = a_n a_{n+1} + 1$. Докажите, что $a_n - 3$ — составное число при $n > 6$.

Занятие 2. Решение сравнений. Теорема Вильсона

Задача 2.1. Пусть $d = \mathrm{НОД}(c, b)$. Докажите, что любое решение сравнения $x \equiv c \pmod b$ делится на d, то есть $x \equiv 0 \pmod d$. При этом x/d является решением сравнения $x/d \equiv c/d \pmod{b/d}$.

Задача 2.2. Пусть b — нечетное число и $2ax \equiv 2c \pmod{b}$. Докажите, что $ax \equiv c \pmod{b}$.

Задача 2.3. Пусть $b \perp k$ (т. е. НОД$(k, b) = 1$). Докажите, что сравнение $axk \equiv ck \pmod{b}$ можно сократить на k: из $axk \equiv ck \pmod{b}$ следует, что $ax \equiv c \pmod{b}$.

Задача 2.4. Докажите, что если $d = \text{НОД}(a, b) > 1$, то сравнение $ax \equiv 0 \pmod{b}$ имеет ненулевое решение.

Задача 2.5. Докажите, что если p — простое число, то:

а) в каждой строке таблицы умножения остатков по модулю p встречается ровно одна единица;

б) единица может стоять на диагонали только в первой и последней строках;

в) числа, сравнимые с 2, 3, 4, ..., $(p-3)$, $(p-2)$ можно разбить на пары так, что произведение чисел в каждой паре будет сравнимо с единицей по модулю p;

г) $(p-1)! \equiv -1 \pmod{p}$.

Задача 2.6 (теорема Вильсона). Докажите, что

$$(p-1)! + 1 \vdots p \Leftrightarrow (p \text{ — простое число}).$$

Задача 2.7. а) Докажите, что если $a \perp b$, то остаток a обратим.

б) Докажите, что если остаток $a \pmod{b}$ обратим, то $a \perp b$.

в) Докажите, что если $a \perp b$, то решением сравнения $ax \equiv c \pmod{b}$ является $c/a \pmod{b}$, то есть $c \cdot (1/a)$.

Задача 2.8. Найдите все решения сравнений: а) $4x \equiv 9 \pmod{13}$; б) $3x \equiv 12 \pmod{15}$; в) $20x \equiv 30 \pmod{55}$.

Задача 2.9. Решите систему сравнений

$$\begin{cases} 6x + 5y \equiv 1 \pmod{11}, \\ 4x + 3y \equiv 2 \pmod{11}. \end{cases}$$

Задача 2.10. а) Докажите, что $(p-2)! \equiv 1 \pmod{p}$ при любом простом p. б) Докажите, что если $(n-2)! \equiv 1 \pmod{n}$, то n — простое.

Задача 2.11. а) Докажите, что если $p = 4k + 1$ — простое число, то $x = ((p-1)/2)!$ удовлетворяет сравнению $x^2 \equiv -1 \pmod{p}$.

б) Найдите хотя бы одно натуральное решение сравнения $x^2 \equiv -1 \pmod{29}$, не превосходящее 28.

Задача 2.12. С помощью теоремы Вильсона докажите, что среди чисел вида $n! + 1$ бесконечно много составных.

Задача 2.13. Пусть $k \geqslant 3$. Найдите все решения сравнения $x^2 \equiv 1 \pmod{2^k}$.

Занятие 3. Леонард Эйлер и его функция

Задача 3.1. Пусть $a \perp m$ и числа $k_1, k_2, \ldots, k_r$ образуют приведённую систему остатков по модулю m. Для каких b числа $ak_i + b$ также образуют приведённую систему остатков по модулю m?

Задача 3.2. а) Чему равно $\varphi(1)$? б) Чему равно $\varphi(p)$, если p — простое число? в) Докажите, что $\varphi(p^2) = p(p-1)$ для простого p.

Задача 3.3. Докажите, что $\varphi(p^n) = p^{n-1}(p-1)$ при любом натуральном n и простом p.

Задача 3.4. Докажите, что функция Эйлера *мультипликативна*: при $a \perp b$ выполнено равенство $\varphi(ab) = \varphi(a)\varphi(b)$.

Задача 3.5. Пусть

$$n = \prod_i p_i^{k_i}$$

— каноническое разложение числа n на простые множители. Выведите из задач 3.3 и 3.4, что

$$\varphi(n) = \prod_i (p_i - 1)p_i^{k_i - 1} = n \prod_i \left(1 - \frac{1}{p_i}\right)$$

(в обоих вариантах формулы произведение берётся по всем простым делителям n).

Задача 3.6. а) Миша выписал все правильные дроби со знаменателем 30 и привёл их все к несократимому виду. Для каждого знаменателя найдите, сколько дробей с этим знаменателем он получил. Докажите, что $30 = \varphi(1) + \varphi(2) + \varphi(3) + \varphi(5) + \varphi(6) + \varphi(10) + \varphi(15) + \varphi(30)$.

б) **(Тождество Гаусса)** Докажите, что любое натуральное число равно сумме значений функции Эйлера для всех его делителей: $n = \sum\limits_{n:d} \varphi(d) = \sum \varphi(d)[n \vdots d]$.

Задача 3.7. Докажите, что $\varphi(m)$ чётно при любом $m > 2$.

Задача 3.8. Докажите, не опираясь на результат задачи 3.5, что: а) $\varphi(m^2) = m\varphi(m)$ для любого натурального m; б) $\varphi(m^k) = m^{k-1}\varphi(m)$ для любых m и k.

Задача 3.9. Докажите, что:

а) $ab = \text{НОД}(a, b)\text{НОК}(a, b)$;

б) $\varphi(a)\varphi(b) = \varphi(\text{НОД}(a, b))\varphi(\text{НОК}(a, b))$;

в) $\varphi(ab)\varphi(\text{НОД}(a, b)) = \varphi(a)\varphi(b)\text{НОД}(a, b)$.

Задача 3.10. Используя формулу для функции Эйлера из задачи 3.4, докажите, что простых чисел бесконечно много.

Задача 3.11. Докажите, что $\varphi(n) = n/2$ тогда и только тогда, когда n — степень двойки.

Задача 3.12. Докажите, что если $n \vdots d$, то $\varphi(n) \vdots \varphi(d)$.

Занятие 4. КТО-КТО в теремочке живёт

Задача 4.1. Докажите, что для любых попарно взаимно простых чисел $m_1, m_2, \ldots, m_n$ и остатков $r_1, r_2, \ldots, r_n$ по модулям m_1, $m_2, \ldots, m_n$ найдутся n последовательных чисел $a, a+1, \ldots, a+n-1$, для которых $a \equiv r_1 \pmod{m_1}$, $a+1 \equiv r_2 \pmod{m_2}$, $\ldots$, $a+n-1 \equiv r_n \pmod{m_n}$.

Задача 4.2. Докажите, что для любого n найдутся n последовательных чисел, делящихся на полные квадраты (отличные от единицы).

Задача 4.3. Натуральное число даёт остаток 3 при делении на 5 и остаток 2 при делении на 7. Какой остаток может оно давать при делении на 35?

Задача 4.4. Пятнадцать простых чисел образуют арифметическую прогрессию с положительной разностью d. Докажите, что $d > 30000$.

Задача 4.5. В китайском календаре используется 12-летний цикл, причём каждому из 12 лет в цикле соответствует одно из животных. Кроме того, каждый год проходит под покровительством одной из пяти стихий и считается окрашенным в цвет этой стихии: годы, оканчивающиеся на 0 и 1, — годы металла (белый цвет), на 2 и 3 — воды (чёрный или синий), на 4 и 5 — дерева (зелёный или бирюзовый), на 6 и 7 — огня (красный), а на 8 и 9 — земли (жёлтый). Таким образом, за 60 лет каждое животное встречается 5 раз, а каждый цвет — 12 раз. Докажите, что в 60-летнем цикле (гань-чжи) возникают все возможные комбинации животных и цветов.

Задача 4.6. Докажите, что числа натурального ряда можно переставить местами так, чтобы сумма любых n первых чисел делилась на n.

Задача 4.7. Докажите, что если натуральный ряд представлен в виде объединения нескольких непересекающихся арифметических прогрессий, то разности любых двух прогрессий имеют общий делитель, больший 1.

Задача 4.8. Найдите наименьшее натуральное число, которое при делении на 3 дает остаток 2, при делении на 5 — остаток 3, при делении на 7 — остаток 2, при делении на 11 — остаток 6.

Задача 4.9. Пусть $f(x)$ — многочлен с целыми коэффициентами. Для $m \geqslant 1$ обозначим через $N_f(m)$ количество различных решений сравнения $f(x) \equiv 0 \pmod{m}$ (решения, отличающиеся на величины, кратные m, будем считать одинаковыми). Докажите,

что функция N_f мультипликативна, т. е.

$$N_f(m_1m_2) = N_f(m_1)N_f(m_2),$$

если $m_1 \perp m_2$.

Задача 4.10. Найдите наименьшее натуральное число, половина которого — квадрат, треть — куб, а пятая часть — пятая степень.

Задача 4.11. При изготовлении елочной гирлянды электрик Петров сделал на куске провода отметки, делящие его на 113 одинаковых кусков, и ушел домой. На следующий день электрик Иванов разметил тот же провод на 137 одинаковых кусков. Наконец, электрик Сидоров разрезал провод по всем отметкам. Куски какого размера у него получились и сколько получилось кусков каждого вида?

Задача 4.12. Докажите, что если бы Сидоров разрезал провод на 250 одинаковых кусков, то на каждом из получившихся кусочков, кроме двух крайних, стояло бы ровно по одной отметке.

Занятие 5. От Ферма к Эйлеру и обратно

Задача 5.1. а) Докажите, что если p — простое число и $0 < a < p$, то $a \cdot 2a \cdot 3a \cdot \ldots \cdot (p-1)a \equiv (p-1)! \pmod{p}$.

б) **(Малая теорема Ферма, МТФ)** Докажите, что если p — простое число и $a \perp p$, то $a^{p-1} \equiv 1 \pmod{p}$.

Задача 5.2. Пусть p простое. Докажите, что если $a^p \equiv b^p \pmod{p}$, то а) $a \equiv b \pmod{p}$; б) $a^p \equiv b^p \pmod{p^2}$.

Задача 5.3. Пусть p простое. Если $m \equiv 1 \pmod{p^d}$, то $m^p \equiv 1 \pmod{p^{d+1}}$.

Задача 5.4 (продолжение задачи 5.3). Если $a^n - b^n$ делится на n, то $(a^n - b^n)/(a-b)$ делится на n.

Задача 5.5. Пусть p — простое число. Докажите, не опираясь на МТФ, что если $m^p \equiv m \pmod{p}$, то $(m+1)^p \equiv (m+1) \pmod{p}$.

Задача 5.6. Пусть p — простое число.

а) **(Тождество Эйзенштейна)** Докажите, что

$$(a+b)^p - a^p - b^p \vdots p.$$

б) Докажите, что $(a_1 + a_2 + \ldots + a_n)^p - a_1^p - a_2^p - \ldots - a_n^p \vdots p$.

Задача 5.7. Найдите остаток от деления а) 2^{100} на 101; б) 2^{900} на 29; в) 28! на 29; г) 56!! на 29.

Задача 5.8. Пусть p — простое число, большее 5. Докажите, что число 11111...11 ($p-1$ единица) делится на p.

Задача 5.9. Докажите, что $16^{2n+1}+(2n+1)^{16} \vdots 17$, если $(2n+1) \perp 17$.

Задача 5.10. Докажите, что если $n \perp 19$, то либо $n^9+1 \vdots 19$, либо $n^9-1 \vdots 19$.

Задача 5.11. Докажите, что если $n \perp 17$, то одно из чисел n^8+1, n^4+1, n^2+1, $n+1$, $n-1$ делится на 17.

Задача 5.12. Докажите, что $17^{120}-1 \vdots 143$.

Занятие 6. Псевдопростые числа и числа Кармайкла

Задача 6.1. Примените тест Ферма для проверки на простоту чисел 511 и 509.

Задача 6.2. Докажите, что если p и q — различные простые числа, то из $a^p \equiv a \pmod q$ и $a^q \equiv a \pmod p$ следует, что $a^{pq} \equiv a \pmod{pq}$.

Задача 6.3. Докажите, что $2^{341} \equiv 2 \pmod{341}$ (при этом $341 = 11 \cdot 31$ — составное число).

Задача 6.4. а) **(Теорема Корсельта)** Докажите, что если $n = p_1p_2...p_k$ и $n-1$ делится на p_i-1 для любого $i=1,...,k$, то n — число Кармайкла, т. е. для любого a выполнено сравнение $a^n \equiv a \pmod n$.

б) Докажите, что $561 = 3 \cdot 11 \cdot 17$ — число Кармайкла.

в) Докажите теорему, обратную теореме Корсельта.

Задача 6.5. Докажите, что: а) 91 — псевдопростое по основанию 3; б) 217 — псевдопростое по основанию 5; в) 645 — псевдопростое по основанию 2; г) 1729 — псевдопростое по основаниям 2, 3 и 5.

Задача 6.6. Докажите, что каждое нечётное число n представимо как разность квадратов соседних натуральных чисел, а каждое нечётное составное число n представимо как разность квадратов двух несоседних чисел, то есть как $(u+k)^2-u^2$ при $k>1$.

Задача 6.7. Докажите, что если n — псевдопростое число по основанию 2, то $M_n = 2^n-1 > n$ — также псевдопростое по основанию 2.

Задача 6.8. Докажите, что: а) если число Мерсенна $M_p = 2^p-1$ составное (при простом p), то оно псевдопростое (по основанию 2); б) если число Ферма $F_p = 2^{2^p}+1$ составное (при простом p), то оно псевдопростое.

Задача 6.9. Псевдопростые числа могут быть чётными. Докажите, что $161038 = 2 \cdot 73 \cdot 1103$ — псевдопростое число (по основанию 2).

Задача 6.10. Докажите, что если числа $6k+1$, $12k+1$ и $18k+1$ простые, то их произведение — число Кармайкла.

Задача 6.11. Докажите, что числами Кармайкла являются: а) $1105 = 5 \cdot 13 \cdot 17$; б) $6601 = 7 \cdot 23 \cdot 41$.

Задача 6.12. Найдите два различных числа Кармайкла вида $n = 13 \cdot 61 \cdot p$, где p — простое число.

Задача 6.13. Докажите, что никакое число Кармайкла не делится на квадрат какого-либо простого числа.

Занятие 7. Шифрование с открытым ключом

Задача 7.1. Найдите ключ дешифровки d для системы асимметричного шифрования, если известно, что $p = 2017$, $e = 13$.

Задача 7.2. Сгенерируйте ключи RSA по следующим исходным данным: $p = 3557$, $q = 2579$, $e = 3$.

Задача 7.3. Протокол Диффи—Хеллмана служит для того, чтобы создавать секретные ключи, пользуясь открытыми (общедоступными, незащищёнными, иначе говоря, ненадёжными) каналами связи. Пусть Алиса и Боб знают два простых числа p и q. Эти числа не секретны, они могут быть известны кому угодно. Чтобы создать общий и неизвестный более никому секретный ключ, Алиса сама генерирует большое случайное число a, а Боб — большое случайное число b. Затем Алиса вычисляет значение $A \equiv q^a \pmod{p}$ и пересылает его Бобу, а Боб вычисляет $B \equiv q^b \pmod{p}$ и пересылает Алисе. Числа A и B называются *открытыми ключами*, потому что предполагается, что пересылка происходит по открытому каналу связи, то есть злоумышленник может перехватить оба этих значения. Затем Алиса на основе имеющегося у неё закрытого ключа a и полученного открытого ключа B вычисляет значение $B^a \pmod{p}$, а Боб аналогично вычисляет $A^b \pmod{p}$. Докажите, что у Алисы и Боба получается одно и то же число. Объясните, почему это число действительно является секретным для всех остальных.

Задача 7.4. Придумайте, как расширить протокол Диффи—Хеллмана на трёх участников — Алису, Боба и Чарли.

Задача 7.5. Придумайте, как использовать протокол Диффи—Хеллмана для шифрования с открытым ключом.

Рекомендуемая литература

1. *Н.В.Алфутова, А.В.Устинов.* Алгебра и теория чисел. Сборник задач. М.: МЦНМО, 2009.

2. *И.М.Виноградов.* Основы теории чисел. СПб.: Лань, 2009.

3. *Р.Крэндалл, К.Померанс.* Простые числа. Криптографические и вычислительные аспекты. М.: URSS, 2011.

4. *А.Р.Лизана.* Гаусс. Теория чисел. Если бы числа могли говорить. М.: Де Агостини, 2015. (Наука. Величайшие теории; Вып. 8).

5. *О.Оре.* Приглашение в теорию чисел. М.: URSS, 2003.

6. *В.В.Прасолов.* Задачи по алгебре, арифметике и анализу. М.: МЦНМО, 2011.

7. *А.И.Сгибнев.* Делимость и простые числа. М.: МЦНМО, 2013.

8. *В.Серпинский.* 250 задач по элементарной теории чисел. М.: Просвещение, 1968.

9. *D.Burton.* Elementary number theory. McGraw-Hill, 2001.

10. *K.Rosen.* Elementary number theory and its applications. Reading, MA: Addison-Wesley, 1984.

11. *J.J.Tattersall.* Elementary number theory in nine chapters. Cambridge: Cambridge University Press, 1999.

Оглавление

Учебно-методическое издание

Константин Александрович Кноп

Азы теории чисел

Серия «Школьные математические кружки»

Подписано в печать 18.01.2017 г. Формат $60 \times 88\,{}^{1}/_{16}$. Бумага офсетная.
Печать офсетная. Объем 5 печ. л. Тираж 3000 экз.

Издательство Московского центра
непрерывного математического образования
119002, Москва, Большой Власьевский пер., 11. Тел. (499) 241-08-04.

Отпечатано в ООО «Типография „Миттель Пресс“».
г. Москва, ул. Руставели, д. 14, стр. 6.
Тел./факс +7 (495) 619-08-30, 647-01-89.
E-mail: mittelpress@mail.ru

Книги издательства МЦНМО можно приобрести в магазине
«Математическая книга», Москва, Большой Власьевский пер., д. 11.
Тел. (495) 745-80-31. E-mail: biblio@mccme.ru

В СЕРИИ «ШКОЛЬНЫЕ МАТЕМАТИЧЕСКИЕ КРУЖКИ»
ВЫШЛИ КНИГИ:

К. А. Кноп. Азы теории чисел

А. Д. Блинков. Геометрия в негеометрических задачах

И. В. Раскина
Логика для всех: от пиратов до мудрецов

А. В. Шаповалов. Математические конструкции:
от хижин к дворцам

А. Д. Блинков, В. М. Гуровиц. Непрерывность

И. В. Раскина, Д. Э. Шноль. Логические задачи

А. А. Заславский, Б. Р. Френкин, А. В. Шаповалов
Задачи о турнирах

А. В. Шаповалов. Как построить пример?

А. И. Сгибнев. Делимость и простые числа

А. Д. Блинков. Классические средние

Г. А. Мерзон, И. В. Ященко.
Длина. Площадь. Объем

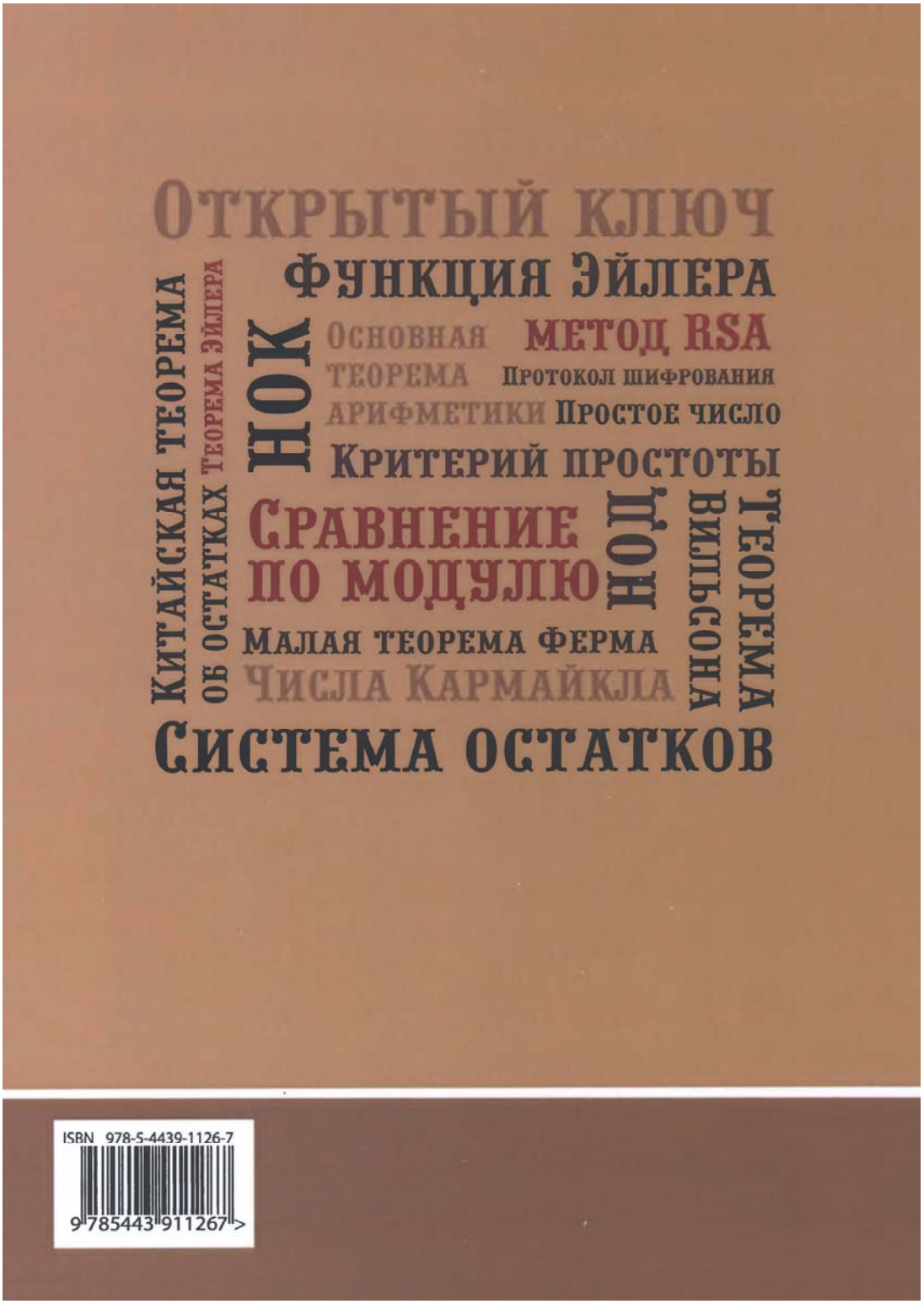
К. А. Кноп.
Взвешивания и алгоритмы: от головоломок к задачам

А. Д. Блинков, Ю. А. Блинков.
Геометрические задачи на построение

П. В. Чулков. Арифметические задачи

В. М. Гуровиц, В. В. Ховрина. Графы

Л. Э. Медников. Чётность



ISBN 978-5-4439-1126-7