

# Азы теории чисел

## Занятие 1. Арифметика остатков



Карл Фридрих Гаусс (30 апреля 1777 – 23 февраля 1855), немецкий математик, астроном и физик. Ещё в детстве проявил яркие способности к математике и иностранным языкам. В 1796 году девятнадцатилетний Гаусс решил задачу, поставленную ещё Евклидом: он нашел способ построить с помощью циркуля и линейки правильный 17-угольник. В 24 года Гаусс опубликовал знаменитые «Арифметические исследования», в которых изложил теорию квадратичных вычетов и сравнений второй степени, а также доказал «квадратичный закон взаимности». Именно в «Арифметических исследованиях» впервые был применён современный язык сравнений, сделавший возможной работу с делимостью чисел как с равенствами. Все догауссовские способы записи фактов о делимости целых чисел были трудночитаемыми и потому неудобными.

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 он по праву заслужил титул «короля математиков».

Фотопортрет К. Гаусса сделан А.Витманом в 1887 году.

Если  $m > 1$  и  $(a-b) : m$ , 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 сравнений, то есть записи  $a \equiv b$  вместо делимости  $(a-b) : m$ , оказывается очень удобным и мощным инструментом в разных задачах, потому что со сравнениями, как мы сейчас убедимся, можно действовать привычно, как с равенствами, то есть складывать, вычитать, умножать, иногда делить.

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

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

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

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  $a^k - b^k = (a-b)(a^{k-1} + a^{k-2}b + \dots + ab^{k-2} + b^{k-1})$ . Другой способ – с помощью математической индукции, многократно применяя произведение сравнений (задачу 1.1б).

Мы будем говорить, что множество  $\mathbf{M}$  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 качестве полной системы остатков выбирается множество  $\{0, 1, 2, \dots, m-1\}$  или множество  $\{1, 2, \dots, m\}$ , а для доказательства того, что какая-то система остатков является полной, для неё устанавливают взаимно однозначное соответствие с одним из двух указанных выше множеств.

**Комментарий:** в этом определении можно заменить условие единственности сравнимого элемента на условие  $|\mathbf{M}|=m$  или даже на  $|\mathbf{M}|\leq m$ . Действительно, если для каждого целого числа есть хотя бы один сравнимый с ним элемент множества, и при этом общее количество элементов  $\mathbf{M}$  не больше  $m$ , то двух различных элементов, сравнимых с одним и тем же числом, быть не может.

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

**Решение.** Сначала докажем простую (почти очевидную) часть этого утверждения. Если  $m : 3$ , то  $m \in \mathbf{M}$ , потому что  $m < 3m-3$ , а  $\mathbf{M}$  содержит все числа, кратные 3 и не превосходящие  $3m-3$ . Но так как  $m \equiv 0 \pmod{m}$ , то  $\mathbf{M}$  содержит хотя бы два различных элемента, сравнимых с числом  $m$  (а именно, 0 и  $m$ ). Следовательно,  $\mathbf{M}$  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):  $\mathbf{M}=\{0, 3, 6, \dots, 3k, 3k+3, \dots, 6k, 6k+3, \dots, 9k\}$ . 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, ...,  $3k-1$ . Точно так же для чисел от  $6k+3$  до  $9k$  выпишем вместо них числа, меньшие их на  $2m=6k+2$  – получатся числа 1, 4, ...,  $3k-2$ . 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.

1.4. Постройте таблицу умножения по mod 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

1.5. Постройте таблицу умножения по mod 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

Предложите ученикам внимательно всмотреться в эти таблицы и вместе ответить на такие вопросы:

- почему в первой таблице не было нулей, а во второй они есть?
- почему в каждой строчке первой таблицы никакое число не повторяется дважды?
- для каких модулей в пределах первого десятка таблицы умножения будут похожи на таблицу mod 5, а для каких — на таблицу mod 6?
- сколько в таблице mod 12 таких строчек, в которых нет нулей?

**Ответы** на эти вопросы:

- 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 mod 6) получается 0.
- 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.
- по-видимому, для простых модулей (то есть чисел 2, 3, 7) таблицы будут аналогичны таблице mod 5 (нет нулей, все числа в каждом столбце и каждой строке различны), а для составных — аналогичны таблице mod 6.
- этот вопрос формулируется так: 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 к занятию 1.

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

Решение.  $6^1+1 = 7$ ,  $6^2+1 \equiv 2+1=3 \pmod{17}$ .. Дальше проще считать сразу «в остатках»,

учитывая предыдущие найденные остатки для степеней шестёрки, перемножая нужные из них и затем добавляя к результату 1:  $6^3+1 \equiv 6 \cdot 2+1 = 13$ ,  $6^4+1 \equiv 2 \cdot 2+1 = 4+1 = 5$ ,  $6^5+1 \equiv 6 \cdot 4+1 \equiv 7+1 = 8$ .

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

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

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

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

1.9. Пусть  $d$  – 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.

**Решение.** 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  $(a'-b') \vdots m'$ . Очевидно, что два таких сравнения равносильны друг другу.

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

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

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

**Решение.** 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  $2014=4 \cdot 503+2$ , то  $7^{2014}=(7^4)^{503} \cdot 7^2 \equiv 1^{503} \cdot 9 \equiv 9 \pmod{10}$ . 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, то какой-то остаток обязательно встретится второй раз. Дальше 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. Докажите, что ни при каком натуральном  $n$  число  $3^n + 5^n$  не является точным квадратом.

**Решение.** Поначалу совершенно непонятно, какое отношение эта задача имеет к сравнениям по модулю. Поэтому начнём с того, что просто сосчитаем несколько первых чисел вида  $3^n + 5^n$ :  $3^1+5^1=8$ ,  $3^2+5^2=34=2 \cdot 17$ ,  $3^3+5^3=152=8 \cdot 19$ ,  $3^4+5^4=706=2 \cdot 353$ ,  $3^5+5^5=3368=8 \cdot 421$ . Возникает гипотеза: при нечётных показателях степени  $3^n + 5^n$  делится на 8, но не делится на 16, а при чётных — делится на 2, но не делится на 4. А так как все точные квадраты содержат чётную

степень двойки, то выражение  $3^n + 5^n$  не может быть точным квадратом. 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, что и доказывает утверждение задачи.

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  $n > 5$ .

**Решение.** 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  $a_8$  было очевидным то, что результат после вычитания 3 не будет простым числом: в результате получались чётные числа. Однако то, что  $528703$  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, и даже с запасом: так как  $a_{n+4} \equiv 3 \pmod{a_n}$ , то  $(a_{n+4} - 3) : a_n$ , причем  $a_n > 1$ . А значит,  $a_{n+4} - 3$  является составным числом.

## Дополнительные задачи к занятию 1

Д1.14. Пусть  $m=2s+1$  – нечётное натуральное число. Докажите, что множество  $\{-s, 1-s, \dots, -1, 0, 1, \dots, s-1, s\}$  – полная система остатков по  $\text{mod } m$ .

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

Д1.15. Докажите, что  $\{0, 1, 2, 2^2, \dots, 2^9\}$  – полная система остатков по  $\text{mod } 11$ .

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

Д1.16. С помощью утверждения задачи 1.10 докажите признаки делимости на а) 9; б) 11.

**Решение.** а) Десятичную запись натурального числа  $\overline{a_n a_{n-1} \dots a_0} = a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \dots + a_0 \cdot 10^0$  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  $10 \equiv 1 \pmod{9}$ , то из 1.11 получаем утверждение о том, что каждое число сравнимо со своей суммой цифр по модулю 9 – а это и есть обобщённый признак делимости на  $9^1$ .

б) знакопеременная сумма цифр  $(-1)^n a_n + (-1)^{n-1} a_{n-1} + a_0$  – это значение этого же самого многочлена в точке  $b=-1$ . Так как  $10 \equiv -1 \pmod{11}$ , то из 1.11 получаем утверждение о том, что каждое число сравнимо со своей знакопеременной суммой цифр по модулю 11.

Д1.17. Пусть  $x, y, z$  – целые числа, удовлетворяющие уравнению  $x^2+y^2=z^2$ . Докажите, что  $xuz \equiv 0 \pmod{60}$ .

<sup>1</sup> Точнее говоря, это признак равноостаточности по модулю 9.

**Решение.** Рассмотрим отдельно делимость  $хуz$  на 3, 4 и 5. Например, рассуждение по mod 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  $1+4 \equiv 0$ , то есть  $z$  делится на 5, откуда сразу получаем, что  $хуz$  делится на 5.

Д1.18. Найдите остатки от деления  $100^{2015}$  на а) 99; б) 101; в) 9999.

**Решение.** а)  $100 \equiv 1 \pmod{99}$ , поэтому  $100^{2015} \equiv 1^{2015} \equiv 1 \pmod{99}$   
б)  $100 \equiv -1 \pmod{101}$ , поэтому  $100^{2015} \equiv (-1)^{2015} \equiv -1 \pmod{101}$ .

Обратите внимание на то, как сравнение с отрицательным числом  $-1$  избавило от выполнения умножений.

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

**Комментарий:** подумайте, как вывести в) из результатов а) и б).

Д1.19. Найдите остаток от деления  $2011 \cdot 2012 \cdot 2013 \cdot 2014 \cdot 2015$  а) на 2010 б) на 2016.

**Решение.** а) Заменяем 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  $0 \leq 120 < 2010$ , 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  $2011 \cdot 2012 \cdot 2013 \cdot 2014 \cdot 2015 \equiv (-5) \cdot (-4) \cdot (-3) \cdot (-2) \cdot (-1) = -120 \pmod{2016}$ . Поэтому искомым остатком будет число  $2016 - 120 = 1896$ .

Д1.20. Докажите, что если  $2^n - 1 : 11$ , то  $2^n - 1 : 93$ .

**Решение.** Здесь снова помогает рассмотрение циклов. По модулю 11:  $2^0=1, 2^1=2, 2^2=4, 2^3=8, 2^4=16 \equiv 5, 2^5=10, 2^6 \equiv 10 \cdot 2 \equiv 9, 2^7 \equiv 9 \cdot 2 \equiv 7, 2^8 \equiv 7 \cdot 2 \equiv 3, 2^9 \equiv 3 \cdot 2 = 6, 2^{10} \equiv 6 \cdot 2 \equiv 1$ . Далее остатки повторяются, поэтому мы делаем вывод о делимости  $2^n - 1$  на 11:  $2^n - 1 \equiv 0 \pmod{11} \Leftrightarrow n : 10$ . 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:  $2^n - 1 \equiv 0 \pmod{31} \Leftrightarrow n : 5$ . 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.

Д1.21. 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.

**Решение.** а) Здесь тоже можно было бы поступить аналогично решению задач 1.6, 1.11, Д1.20 и сосчитать несколько первых остатков (до заикливания), 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  $3^{100} = (3^4)^{25} = (-2^4)^{25} = -2^{100} \pmod{97}$ , 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  $p=3^5-2^5=211$ .

Д1.22. Докажите, что  $(3^n - 1)^n - 4 \equiv 3^n - 4 \pmod{3^n - 4}$  при любом натуральном  $n$ .

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

Д1.23. Найдите все нечётные натуральные делители числа  $5^{2n} + 3 \cdot 2^{5n-2}$ .

**Решение.**  $5^{2n} + 3 \cdot 2^{5n-2} = 25 \cdot 2^{5n-2} + 3 \cdot 2^{5n-2} = 28 \cdot 2^{5n-2} = 7 \cdot 2^{5n}$ . Нечётными делителями такого числа являются только 1 и 7.

Д1.24. Докажите, что а)  $3^{n+2} + 4^{2n+1} \equiv 0 \pmod{13}$ . б)  $6^{n+2} + 7^{2n+1} \equiv 43 \pmod{43}$ . в)  $k^{n+2} + (k+1)^{2n+1} \equiv k^2 + k + 1 \pmod{k^2 + k + 1}$

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

б) как и а), является частным случаем задачи в).

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

Д1.25. Докажите, что  $2^{5n+1} + 5^{n+2} \equiv 27 \pmod{27}$ .

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

Д1.26. Докажите, что если  $a$  – нечётное число, а  $n$  – натуральное, то  $a^{2^n} \equiv 1 \pmod{2^{n+2}}$ .

**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.

Д1.27. Число  $a$  заканчивается на 33. На какие две цифры заканчивается  $a^{85}$ ?

**Указание:** умножать число 33 на себя 85 раз — не лучшая идея, и искать цикл по mod 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  $a^2 = 33 \cdot 33 = 1089 \equiv -11 \pmod{100}$ ,  $a^4 = (-11) \cdot (-11) \equiv 21 \pmod{100}$ ,  $a^8 = a^4 \cdot a^4 \equiv 21 \cdot 21 \equiv 41 \pmod{100}$ ,  $a^{16} = a^8 \cdot a^8 \equiv 41 \cdot 41 \equiv 81 \pmod{100}$ ,  $a^{17} = a \cdot a^{16} \equiv 33 \cdot 81 \equiv 73 \pmod{100}$ ,  $a^{34} = a^{17} \cdot a^{17} \equiv 73 \cdot 73 \equiv 29 \pmod{100}$ ,  $a^{68} \equiv 29 \cdot 29 \equiv 41 \pmod{100}$ ,  $a^{85} = a^{68} \cdot a^{17} \equiv 41 \cdot 73 \equiv 93 \pmod{100}$

**Комментарий 1:** Нам хватило всего 8 умножений, а цикл имеет длину 20, поэтому если бы досчитывать все степени подряд до появления цикла, то вычислительной работы было бы больше.

**Комментарий 2:** Набор промежуточных степеней вместо у нас был таким: 2, 4, 8, 16, 17, 34, 68. Иначе говоря, мы нашли сначала 17 – наибольший простой делитель 85, а затем вычисляли его квадрат и четвертую степень. Можно было бы пойти и через другой простой делитель, то есть вычислить 2, 4, 5, 10, 20, 40, 80 степени и затем уже использовать  $85 = 80+5$ . 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  $a^{32} \equiv 81 \cdot 81 \equiv 61 \pmod{100}$ ,  $a^{64} \equiv 61 \cdot 61 \equiv 21 \pmod{100}$ . Теперь осталось перемножить нужные степени  $a$ :  $a^{85} = a \cdot a^4 \cdot a^{16} \cdot a^{64} \equiv 33 \cdot 21 \cdot 81 \cdot 21 \equiv 93 \pmod{100}$



**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, требуемых 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).

Д1.28. Найдите три последних цифры числа  $7^{2016}$ .

**Решение.**  $7^4 \equiv 401 \pmod{1000}$ , поэтому  $7^{4n} \equiv (1+400)^n \equiv 1+400n$ . Так как  $2016=4 \cdot 504$ , а  $1+400 \cdot 504 = 601 \pmod{1000}$ , то  $7^{2016}$  заканчивается на 601.

Д1.29. Найдите все значения  $n$ , для которых  $1!+2!+\dots+n!$  — точный квадрат.

**Решение.** При  $n \leq 4$  точных квадратов нет. При  $n \geq 5$   $1!+2!+3!+4! + \dots + n! \equiv 1!+2!+3!+4! \equiv 5 \pmod{10}$ , поэтому точным квадратом сумма может быть только если она заканчивается на 25. Но так как по модулю 4 сумма всех последующих факториалов равна 3, то заканчиваться на 25 она не может.

Д1.30. Пусть  $m$  — чётное число. Докажите, что если  $\{a_1, a_2, \dots, a_m\}$  и  $\{b_1, b_2, \dots, b_m\}$  — две полные системы остатков по модулю  $m$ , то  $\{a_1+b_1, a_2+b_2, \dots, a_m+b_m\}$  не является полной системой остатков по модулю  $m$ .

**Решение.** Предположим противное. Тогда  $1+2+\dots+m \equiv (a_1+b_1)+(a_2+b_2)+\dots+(a_m+b_m) = (a_1+a_2+\dots+a_m) + (b_1+b_2+\dots+b_m) \equiv 2(1+2+\dots+m) \pmod{m}$ . Отсюда получается, что  $1+2+\dots+m \equiv 0 \pmod{m}$ , то есть  $m(m+1)/2 \equiv 0 \pmod{m}$ , что невозможно при чётном  $m$ . Противоречие.

Д1.31. [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  $m=n$ .

**Решение.** Если  $k$  — делитель  $n$ , то  $n/k$  — тоже делитель  $n$ . Если  $d_1, d_2, \dots, d_s$  — все делители числа  $n$ , а  $e_1, e_2, \dots, e_t$  — все делители числа  $m$ , то имеем  $d_1+d_2+\dots+d_s=n(1/d_1+1/d_2+\dots+1/d_s)$  и  $e_1+e_2+\dots+e_t=m(1/e_1+1/e_2+\dots+1/e_t)$ . Приравнивая левые части и учитывая, что  $1/d_1+1/d_2+\dots+1/d_s=1/e_1+1/e_2+\dots+1/e_t$  (по условию), получаем  $m=n$ .

<http://www.ashap.info/Knigi/Matkruzhki/index.html>