Раздел 19. ЭЛЕМЕНТЫ ТЕОРИИ ЧИСЕЛ И ПРИКЛАДНОЙ АЛГЕБРЫ

> Раньше теория чисел рассматривалась как элегантная, но почти бесполезная область чистой математики. В наши дни теоретико-числовые алгоритмы нашли широкое применение. В определенной степени это произошло благодаря изобретению криптографических схем, основанных на больших простых числах. Применимость этих схем базируется на том, что имеется возможность легко находить большие простые числа, а их безопасность – на отсутствии простой возможности разложения на множители произведения больших простых чисел.
>
> *Т. Кормен, Ч. Лейзерсон, Р. Ривест, К. Штайн*
> *«Алгоритмы: построение и анализ»* (2005)

Элементарная теория чисел занимается изучением свойств целых чисел. Несмотря на простоту объекта исследования, эта область содержит много нетривиальных задач и имеет интересные приложения. В конце XX в. с появлением криптосистем Диффи – Хеллмана и RSA теория чисел стала интенсивно использоваться в криптографии. По некоторым оценкам, в настоящее время практически весь мировой парк средств асимметричной криптографии в математическом плане основан на теоретико-числовых задачах. В теории чисел существует много задач, которые достаточно просто формулируются, однако до сих пор не решены. Неразрешимость или трудноразрешимость некоторых из них является залогом безопасности современных криптосистем.

§ 1. Целые числа. Основная теорема арифметики

Множество целых чисел обозначают

$$\mathbb{Z} = \{0; \pm 1; \pm 2; \ldots; \pm n; \ldots\}.$$

Натуральными называются числа, которые используются при счете; ***множество натуральных чисел*** обозначают

$$\mathbb{N} = \{1; 2; \ldots; n; \ldots\}.$$

На множестве целых чисел определены операции сложения и умножения, а также операция вычитания как обратная к операции сложения. Сумма, разность и произведение двух целых чисел все-

гда являются целым числом. Результат деления двух целых чисел не всегда является целым числом.

Опр. 1. Если для целых чисел a и b, где $b \neq 0$, существуют целые числа q и r такие, что

$$a = b \cdot q + r, \text{ где } 0 \le r < |b|,$$

то r называют ***остатком***, а q – ***частным*** (***неполным частным*** при $r \neq 0$) от деления a на b.

Т 1 (о делении с остатком). Для любых целых чисел a и b, где $b \neq 0$, существуют единственные целые числа q и r такие, что

$$a = b \cdot q + r, \text{ где } 0 \le r < |b|.$$

Пример 1.

1) $a = 37, b = 15$. Поскольку $37 = 15 \cdot 2 + 7$, то $q = 2, r = 7$.

2) $a = -26, b = 4$. Поскольку $-26 = 4 \cdot (-7) + 2$, то $q = -7, r = 2$.

3) $a = 22, b = -5$. Поскольку $22 = -5 \cdot (-4) + 2$, то $q = -4, r = 2$.

4) $a = -15, b = -6$. Поскольку $-15 = -6 \cdot 3 + 3$, то $q = 3, r = 3$. •

Опр. 2. Если остаток от деления a на b равен 0 ($r = 0$), т. е. $a = b \cdot q$, то говорят,

- что a ***делится на*** b ***и на*** q (и пишут $a \vdots b, a \vdots q$);
- что a является ***кратным*** чисел b и q;
- что b и q ***делят*** a (и пишут $b \mid a, q \mid a$);
- что b и q являются ***делителями*** (или ***множителями***) числа a.

Будем обозначать $b \nmid a$, если b не делит a.

Число 0 делится на любое целое число $b \neq 0$.

Любое целое число $a \neq 0$ делится на $1; -1; a; -a$. В дальнейшем будем говорить только о *целых положительных*, т. е. *натуральных делителях*.

Простые и составные числа

Опр. 3. Натуральное число $n > 1$ называется ***простым***, если оно делится только на 1 и на само себя, в противном случае n называется ***составным***.

Замечание. Число 1 не является ни простым, ни составным. Таким образом,

$$\mathbb{N} = \{1\} \cup \{\text{простые числа}\} \cup \{\text{составные числа}\}.$$

Т 2 [Евклид, III в. до н. э.]. Простых чисел бесконечно много.

Доказательство проводится методом «от противного». Допустим, что утверждение теоремы неверно и множество простых чисел конечно. Пусть $p_1, p_2, ..., p_k$ – все простые числа. Рассмотрим число $N = p_1 p_2 ... p_k + 1$. Число N не делится ни на одно из чисел $p_i, i = \overline{1,k}$, так как в противном случае $p_i \mid 1$ (в силу свойства 1 делимости целых чисел). Поэтому либо N является простым числом (не вошедшим в приведенный выше список), либо N – составное и тогда имеется $p \mid N$, где p – отличное от p_i простое число.

Таким образом, пришли к противоречию с предположением, что множество простых чисел содержит только числа $p_1, p_2, ..., p_k$, что доказывает справедливость утверждения теоремы. ◁

Рассуждение Евклида укладывается в одну фразу: если бы имелось лишь конечное число простых чисел, то можно было бы их перемножить и, прибавив единицу, получить число, которое не делится ни на одно простое, что невозможно.

Упражнение 1. Верно ли, что все числа вида $N = p_1 p_2 ... p_k + 1$ являются простыми?

Т 3 (Основная теорема арифметики). Всякое натуральное число $n > 1$ однозначно раскладывается в произведение простых чисел с точностью до порядка следования множителей:

$$n = p_1 p_2 \dots p_s.$$

Если в разложении натурального числа на простые множители собрать одинаковые множители, то получим ***каноническое разложение*** натурального числа:

$$n = p_1^{r_1} p_2^{r_2} \dots p_t^{r_t}.$$

Каноническим разложением целого отрицательного числа $z = -n$ считается, соответственно, его представление в виде $z = -p_1^{r_1} ... p_t^{r_t}$.

Пример 2.

1) $-196 = (-2) \cdot 98 = (-2) \cdot 2 \cdot 49 = -2^2 \cdot 7^2$;

2) $2^{12} - 1 = 4095 = 3^2 \cdot 5 \cdot 7 \cdot 13$. •

Понятие о задачах распознавания простых чисел и факторизации целых чисел

Для целей криптографии (как для практической реализации и обоснования стойкости криптографических средств, так и для разработки методов их вскрытия) необходимо разрабатывать эффективные методы и алгоритмы:

• проверки простоты целых чисел;

• поиска больших простых чисел (в криптографии используются большие простые числа длиной более 80–90 десятичных знаков);

• факторизации целых чисел.

Факторизацией натурального числа называется разложение этого числа в произведение простых сомножителей. Эта задача имеет большую вычислительную сложность. Один из самых популярных методов криптографии с открытым ключом, метод RSA, основан на трудоемкости задачи факторизации длинных целых чисел.

WWW ВИКИСПРАВКА WWWWWWWWWWWWWWWWWWWWWW

На момент опубликования в 1977 г. алгоритма RSA было известно лишь небольшое количество алгоритмов факторизации, которые позволяли на тот день факторизовать числа, состоящие не более чем из 25–30 цифр. Поэтому использование натурального числа, имеющего более 100 десятичных знаков, гарантированно обеспечивало безопасность шифрования этим методом. Сами создатели метода предложили всей математической общественности для тестового взлома 129-значное десятичное число, пообещав за его разложение условное вознаграждение в $100:

N = 114 381 625 757 888 867 669 235 779 976 146 612 010 218
296 721 242 362 562 561 842 935 706 935 245 733 897 830 597
123 563 958 705 058 989 075 147 599 290 026 879 543 541.

История с разложением 129-значного числа создателей метода RSA закончилась в 1994 г., когда с помощью алгоритма квадратичного решета, реализованного в сети коллективом авторов, возглавляемым А. Ленстрой, было выполнено разложение этого числа на сомножители. Данная процедура потребовала колоссальных усилий. Была задействована сеть, состоящая из 1600 компьютеров, которые, проработав 220 дней, подготовили систему линейных уравнений, содержащую более 0,5 млн неизвестных. Потом эта система была решена с помощью суперкомпьютера за 2 дня вычислений.

В 1991 г. по инициативе RSA Laboratories был объявлен конкурс RSA Fac-

toring Challenge, который заключался в разложении на множители больших чисел, каждое из которых представляло собой произведение двух простых множителей. Для разложения было предложено 54 числа длиной от 100 до 617 десятичных знаков. Официально конкурс завершился в 2007 г., однако в августе 2018 г. было разложено только 20 из 54 чисел.

W W W W W W W W W W W W W W W W W W W W W W W W W W W W W W

В настоящее время исследования в области построения быстрых алгоритмов факторизации интенсивно ведутся во всем мире. Ежегодно проводятся десятки конференций по этой тематике, достигаются новые рекорды факторизации длинных чисел, исследуются известные проблемы алгоритмической теории чисел и ставятся новые проблемы.

Авторы книги «Простые числа: Криптографические и вычислительные аспекты» (2-е изд., 2005, цитируется по русскому изданию 2011 г.) Р. Крэндалл и К. Померанс так описывают прогресс в области факторизации и проверки простоты целых чисел:

«Сейчас мы можем разлагать на множители числа, количество знаков в которых в восемь раз больше, чем 30 лет назад, а количество знаков в числах, простоту которых мы можем запросто распознать, примерно в 500 раз больше.

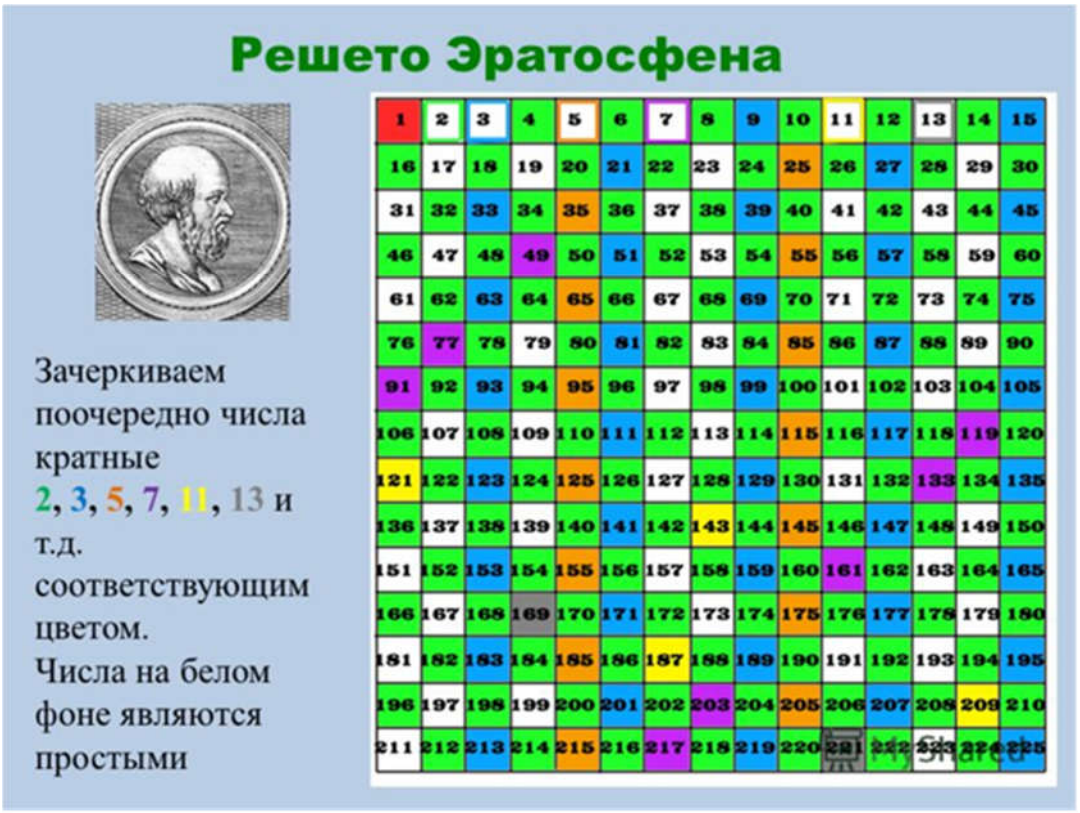
Обратим внимание читателя на тот факт, что вычислительный прогресс имеет две стороны: технологическую и алгоритмическую. Несомненно, надо отдать должное качеству и количеству вычислительной техники, но, что также несомненно, не в полной мере. Если бы мы до сих пор использовали алгоритмы, созданные до 1975 г., то даже с помощью наилучшего доступного сегодня оборудования мы не смогли бы разложить на множители или установить простоту числа, состоящего более чем из 40 знаков.

Итак, что же возможно в наши дни? Текущий рекорд для разложения на множители произвольных чисел – более 170 знаков, а проверить на простоту сегодня можно любое число вплоть до $10^{15\,000}$.»

На настоящий момент не известны *полиномиальные алгоритмы* факторизации чисел, хотя и не доказано, что таких алгоритмов не существует. На предполагаемой большой вычислительной сложности задачи факторизации базируется криптосистема RSA и некоторые др.. Факторизация с полиномиальной сложностью теоретически возможна на квантовом компьютере с помощью алгоритма Шора.

Простейшие методы проверки простоты целых чисел

1. «Решето Эратосфена» – метод получения всех простых чисел на отрезке натурального ряда от 2 до *n*, а также метод проверки числа *n* на простоту путем вычеркивания всех чисел, кратных 2, 3, 5, 7, 11, 13 и т. д. (вычеркиваем, начиная с 2, каждое второе число, т. е. все числа, кратные 2; первое незачеркнутое число – простое число 3, вычеркиваем 3 и дальше каждое третье число, а значит, все числа, кратные 3; первое незачеркнутое число – простое число 5, вычеркиваем все числа, кратные 5 и т. д.)



W W W В И К И С П Р А В К А W W W W W W W W W W W W W W W W W W W W W W W W

Эратосфе́н Кире́нский
(др.-греч. Ἐρατοσθένης ὁ Κυρηναῖος)
(276 год до н. э. – 194 год до н. э.)
греческий математик, астроном, географ, филолог и поэт; с 235 г. до н. э. глава Александрийской библиотеки.
Один из самых разносторонних ученых античности, за энциклопедическую эрудированность современники прозвали его Πένταθλος, т. е. «Пятиборец».
Считается основоположником научной географии и хронологии. Предложил метод определения величины диаметра Земли, его результат был первым достаточно точным расчетом размеров нашей планеты.

Замечание. Достаточно вычеркнуть все числа, кратные простым числам от 2 до $\sqrt{n}$.

Утв. 1. Если натуральное число $n>1$ не делится ни на одно простое $p \le \sqrt{n}$, то число *n* простое.

Упражнение 2. Почему $p \le \sqrt{n}$?

Замечание. Для реализации метода нужен большой объем памяти ЭВМ, однако для составления таблиц простых чисел он является наилучшим.

2. Метод пробных делений является наиболее элементарным методом проверки простоты натурального числа *n* или нахождения его делителей. Он также основан на теореме 3 и заключается в последовательных попытках деления числа *n* на 2 и все нечетные числа от 3 до $\sqrt{n}$.

Замечание. Поскольку, очевидно, все простые числа, кроме 2 и 3, имеют вид $6k+1$ или $6k+5$, то последовательность возможных делителей, превосходящих 3, можно получить, начав с числа 5 и добавляя к пробному делителю попеременно то 2, то 4.

В книге Р. Крэндалла и К. Померанса «Простые числа: Криптографические и вычислительные аспекты» (2-е изд., 2005, русский перевод – 2011 г.) дается следующая оценка скорости работы этого алгоритма на современных устройствах: «Говоря очень приблизительно, современная рабочая станция позволяет за одну минуту распознать методом пробных делений простые числа, состоящие не более чем из 13 десятичных разрядов, а за сутки, быть может, удастся исследовать и 19-значное число».

Алгоритм пробных делений имеет *экспоненциальную оценку сложности* относительно длины входного числа, поэтому этот метод не может быть использован для тестирования больших чисел. Однако пробные деления на числа от 2 до некоторого B проводятся, как правило, на предварительном этапе более сложных и эффективных современных алгоритмов.

Существует множество полиномиальных (относительно длины числа) тестов простоты, но большинство из них являются вероятностными (например, тест Миллера – Рабина). В 2002 г. было доказано, что задача проверки на простоту в общем виде полиномиально разрешима, но предложенный детерминированный тест Агравала – Каяла – Саксены имеет довольно большую вычислительную сложность, что затрудняет его практическое применение.

Для некоторых классов чисел существуют эффективные специальные тесты простоты.

Числа Мерсенна

Числа Мерсенна – это числа вида $2^p - 1$. Числа Мерсенна были открыты в результате поиска совершенных чисел (***совершенными*** называются натуральные числа, которые равны сумме всех своих делителей, меньших данного числа, например, 6 = 1 + 2 + 3; первые четыре совершенных числа – это 6; 28; 496; 8128).

Одним из свойств чисел Мерсенна является то, что числа такого вида могут быть простыми только тогда, когда p – простое число. Однако не для любого простого p число $2^p - 1$ является простым, например, $2^{11} - 1 = 2047 = 23 \cdot 89$.

WWW ВИКИСПРАВКА WWWWWWWWWWWWWWWWWWWWWW

Марéн Мерсéнн
(фр. *Marin Mersenne)*
(1588–1648)
французский математик, физик, философ и богослов, теоретик музыки.
На протяжении первой половины XVII в. был по существу координатором научной жизни Европы, ведя активную переписку практически со всеми видными учеными того времени (78 корреспондентов, в числе которых Декарт, Галилей, Кавальери, Паскаль, Роберваль, Торричелли, Ферма, Гюйгенс и др.).
Живя в Париже, еженедельно собирал математиков и физиков для обсуж-

дения научных результатов и идей. Позднее из этого кружка образовалась Парижская академия наук.
Имеет также серьезные личные научные заслуги в области математики, акустики и теории музыки.

W W W W W W W W W W W W W W W W W W W W W W W W W W W W W W W W W

Числа Мерсенна получили известность в связи с эффективным критерием простоты Люка – Лемера, благодаря которому простые числа Мерсенна давно удерживают лидерство как самые большие известные простые числа. Этот тест был придуман Люка (Lucas) в 1878 г. и усовершенствован Лемером (Lehmer) в 1930 г. Еще в 1876 г. Люка с помощью данного критерия установил, что число

$$2^{127} - 1 = 170\,141\,183\,460\,469\,231\,731\,687\,303\,715\,884\,105\,727$$

является простым. Это число оставалось самым большим известным простым числом на протяжении 75 лет.

W W W В И К И С П Р А В К А W W W W W W W W W W W W W W W W W W W W W

Поиском простых чисел Мерсенна занимается проект распределенных вычислений GIMPS (Great Internet Mersenne Primes Search), организованный в 1995 г. Именно участники этого проекта последнее время находят простые числа Мерсенна. Инструментом поиска служит программа Prime95 Джорджа Вольтмана, где и используется тест Люка – Лемера. Исходный текст этой программы открыт для изучения и представляет собой высоко оптимизированный ассемблерный код.
38-е простое число Мерсенна, открытое в 1999 г., являлось самым большим простым числом на конец XX в., – это число $2^{6\,972\,593} - 1$, которое содержит 2 098 960 десятичных знаков. К настоящему времени известны первые 48 и еще 3 простых числа Мерсенна (не завершена проверка простоты некоторых чисел Мерсенна между найденными). Примечательно, что 45-е простое число Мерсенна было найдено на две недели позже 47-го простого числа Мерсенна, а 46-е было найдено только через год.
За нахождение 47-го простого числа Мерсенна проектом GIMPS в 2009 г. была получена премия в 100 тыс. долл. США, назначенная сообществом Electronic Frontier Foundation за нахождение простого числа, десятичная запись которого содержит не менее 10 млн цифр.

Список известных простых чисел Мерсенна

$2^2 - 1$	$2^3 - 1$	$2^5 - 1$	$2^7 - 1$
$2^{13} - 1$	$2^{17} - 1$	$2^{19} - 1$	$2^{31} - 1$
$2^{61} - 1$	$2^{89} - 1$	$2^{107} - 1$	$2^{127} - 1$
$2^{521} - 1$	$2^{607} - 1$	$2^{1\,279} - 1$	$2^{2\,203} - 1$
$2^{2\,281} - 1$	$2^{3\,217} - 1$	$2^{4\,253} - 1$	$2^{4\,423} - 1$
$2^{9\,869} - 1$	$2^{9\,941} - 1$	$2^{11\,213} - 1$	$2^{19\,937} - 1$

$2^{21\,701}-1$	$2^{23\,209}-1$	$2^{44\,497}-1$	$2^{86\,243}-1$
$2^{110\,503}-1$	$2^{132\,049}-1$	$2^{216\,091}-1$	$2^{756\,839}-1$
$2^{859\,433}-1$	$2^{1\,257\,787}-1$	$2^{1\,398\,269}-1$	$2^{2\,976\,221}-1$
$2^{3\,021\,377}-1$	$2^{6\,972\,593}-1$	$2^{13\,466\,917}-1$	$2^{20\,996\,011}-1$
$2^{24\,036\,583}-1$	$2^{25\,964\,951}-1$	$2^{30\,402\,457}-1$	$2^{32\,582\,657}-1$
$2^{37\,156\,667}-1$	$2^{42\,643\,801}-1$	$2^{43\,112\,609}-1$	$2^{57\,885\,161}-1$
$2^{74\,207\,281}-1$	$2^{77\,232\,917}-1$	$2^{82\,589\,933}-1$	

21 декабря 2018 г. наибольшим известным простым числом стало число $2^{82\,589\,933}-1$, которое содержит 24 862 048 десятичных цифр. По состоянию на сентябрь 2021 г., 8 наибольших простых чисел – это числа Мерсенна. На 9-м месте стоит число, найденное в рамках проекта PrimeGrid, целью которого является поиск различных простых чисел специального вида, а также исследование отрытых проблем теории чисел.

W W W W W W W W W W W W W W W W W W W W W W W W W W W W W W

Некоторые факты о простых числах

Эйлером был получен следующий любопытный результат, который еще раз доказывает бесконечность множества простых чисел.

Т 4 [Эйлер, 1737]. Ряд $\frac{1}{2}+\frac{1}{3}+\frac{1}{5}+\frac{1}{7}+\frac{1}{11}+\dots$ из обратных к простым числам величин является расходящимся.

Это означает, что сумма ряда равна ∞. Тем не менее, *частичная сумма по всем известным на данный момент простым числам не превышает 20*. (Доказано, что $\sum_{p<N}\frac{1}{p}=\ln\ln N+0,26149+\varepsilon(N)$, где $\varepsilon(N)\to 0$ при $N\to\infty$.)

Значение простых чисел в том, что они, согласно Основной теореме арифметики, являются составными элементами всех натуральных чисел. Распределение простых чисел среди натуральных достаточно непредсказуемо. Например, в первой сотне натуральных чисел их 25, во второй – 21, в третьей – 16 и т. д. В первой тысяче натуральных чисел 168 простых, во второй – 135, в третьей – 120 и т. д.

В теории чисел изучается функция $\pi(x)$, выражающая количество простых чисел, меньших либо равных x.

Т 5 [Чебышев, 1849]. Справедлива оценка

$$A\frac{x}{\ln x}\le\pi(x)\le B\frac{x}{\ln x},\ \text{где}\ A\approx 0,921,\ B\approx 1,106.$$

Для распределения простых чисел справедливы также следующие любопытные факты.

Т 6 [Чебышев, 1850]. Между числами k и $2k$, $k>1$, обязательно найдутся простые.

Т 7. Для всякого натурального n существует отрезок $[k;k+n]$, $k\in\mathbb{N}$, натурального ряда, все числа которого составные.

В самом деле, все следующие числа составные:

$$k=(n+2)!+2;\quad ...;\quad k+n=(n+2)!+n+2$$

(здесь $k!=1\cdot 2\cdot 3\ldots\cdot k$, $k\in\mathbb{N}$, 0! = 1).

Т 8 [Дирихле, 1837]. Всякая арифметическая прогрессия $\{a+bn\}$, где числа a и b – заданные взаимно простые натуральные числа, содержит бесконечно много простых чисел.

§ 2. НОД и НОК. Алгоритм Евклида. Соотношение Безу

Опр. 1. Максимальный из общих делителей целых чисел $a_1,a_2,\ldots,a_n$ называется их ***наибольшим общим делителем*** (***НОД***) и обозначается: НОД$(a_1,a_2,\ldots,a_n)$ или $(a_1,a_2,\ldots,a_n)$.

Опр. 2. Минимальное натуральное из общих кратных целых чисел $a_1,a_2,\ldots,a_n$ называется их ***наименьшим общим кратным*** (***НОК***) и обозначается: НОК$(a_1,a_2,\ldots,a_n)$ или $[a_1,a_2,\ldots,a_n]$.

Утв. 1. Если канонические разложения двух чисел имеют вид

$$a=p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_s^{\alpha_s},\ b=p_1^{\beta_1}p_2^{\beta_2}\ldots p_s^{\beta_s},\ \text{где}\ \alpha_i,\beta_i\geq 0,$$

то

$$(a,b)=p_1^{\gamma_1}p_2^{\gamma_2}\ldots p_s^{\gamma_s},\ \text{где}\ \gamma_i=\min\{\alpha_i,\beta_i\};$$

$$[a,b]=p_1^{\delta_1}p_2^{\delta_2}\ldots p_s^{\delta_s},\ \text{где}\ \delta_i=\max\{\alpha_i,\beta_i\}.$$

Пример 1. Найдем (168,180) и [168,180].

Решение. Поскольку

$$168=2\cdot 84=2\cdot 2\cdot 42=2\cdot 2\cdot 2\cdot 21=2\cdot 2\cdot 2\cdot 3\cdot 7=2^3\cdot 3\cdot 7;$$
$$180=2\cdot 90=2\cdot 2\cdot 45=2\cdot 2\cdot 3\cdot 15=2\cdot 2\cdot 3\cdot 3\cdot 5=2^2\cdot 3^2\cdot 5,$$

то

$$(168,180)=2^2\cdot 3^1\cdot 5^0\cdot 7^0=12;$$

$$[168,180]=2^3\cdot 3^2\cdot 5^1\cdot 7^1=2520.\ \bullet$$

Т 1. НОК и НОД двух целых чисел связаны соотношением:

$$[a,b](a,b)=ab.$$

Доказательство. Если $d=(a,b)$, то $a=a_1d$, $b=b_1d$, где $(a_1,b_1)=1$. Тогда

$$[a,b]=a_1b_1d=\frac{ab}{d}=\frac{ab}{(a,b)},$$

что и доказывает теорему. ◁

Опр. 3. Целые числа a и b называются ***взаимно простыми***, если $(a,b)=1$. (Другими словами, это числа, не имеющие общих простых делителей.)

Пример 2. Числа 6 и 35 взаимно просты, так как (6,35) = 1, но 6 и 27 не являются взаимно простыми, так как (6,27) = 3.•

Замечание. Число 1 взаимно просто с любым целым числом; число 0 взаимно просто только с 1 и -1.

Т 2. Если $a=bq+r$, то $(a,b)=(b,r)$.

Доказательство. Пусть $(a,b)=d,(b,r)=k$.

По свойству делимости, если $d\mid a$ и $d\mid b$, то $d\mid r$. Следовательно, $d\mid k$.

С другой стороны, если $k\mid b$ и $k\mid r$, то $k\mid a$. Следовательно, $k\mid d$.

Поскольку $d\mid k$ и $k\mid d$, причем $d,k>0$, то $d=k$ и теорема доказана. ◁

На этой теореме основывается алгоритм Евклида.

Алгоритм Евклида

Алгоритм Евклида – алгоритм для определения НОД двух чисел путем последовательного применения теоремы о делении с остатком.

Т 3. Наибольший общий делитель целых чисел a и b (где $a\nmid b$, $b\nmid a$, $|a|>|b|$) равен последнему отличному от нуля остатку от деления в цепочке равенств:

$$a=bq_1+r_1;$$
$$b=r_1q_2+r_2,\ \text{если}\ r_1\neq 0;$$

$$\ldots;$$
$$r_{n-2} = r_{n-1}q_n + r_n, \text{ если } r_{n-1} \neq 0;$$
$$r_{n-1} = r_n q_{n+1}, \text{ если } r_n \neq 0,$$

т. е. $r_n = (a,b)$.

Доказательство. Согласно теореме 2 и поскольку $r_n > 0$ как остаток от деления, имеем

$$(a,b) = (b,r_1) = (r_1,r_2) = \ldots = (r_{n-1},r_n) = r_n.$$

Процесс получения (a,b) конечен, поскольку мы оперируем только с целыми числами и, начиная с деления r_1 на r_2, – с целыми положительными числами. При этом идет постоянное уменьшение остатков $r_i : 0 \le r_i < r_{i-1}$, поэтому за конечное число шагов будет достигнут остаток $r_{n+1} = 0$. ◁

Алгоритм Евклида известен из «Начал» Евклида, написанных около 300 года до н. э. По всей вероятности, алгоритм не был открыт Евклидом, а появился почти на 200 лет раньше. Евклид формулировал проблему геометрически как задачу нахождения общей «меры» для двух отрезков, и его алгоритм состоял в последовательном вычитании меньшего отрезка из большего.

Замечание. Алгоритм Евклида является одним из старейших известных алгоритмов, но остается в классе самых быстрых алгоритмов нахождения НОД целых чисел.

Пример 3. Найдем (72,26).

Решение.

$$72 = 26 \cdot 2 + 20;$$
$$26 = 20 \cdot 1 + 6;$$
$$20 = 6 \cdot 3 + 2;$$
$$6 = 2 \cdot 3.$$

Следовательно, (72,26) = 2.●

Замечание. Обратное применение цепочки равенств алгоритма теоремы 3 доказывает следующий факт.

Т 4. Если $d = (a, b)$, то существуют такие целые u и v, что выполняется следующее соотношение:

$$d = ua + vb.$$

Замечание. НОД(a, b) является наименьшим натуральным числом, которое может быть представлено в виде линейной комбинации чисел a и b с целыми коэффициентами.

Упражнение 1. Почему?

Опр. 4. Полученное равенство называют ***линейным разложением,*** или ***соотношением Безу*** для наибольшего общего делителя целых чисел a и b, а числа u и v – ***коэффициентами Безу***.

Пример 4. Найдем соотношение Безу для (72, 26).

Решение. Из примера 3 следует, что

$$\begin{gathered} 2 = 20 + 6\cdot(-3) = \\ = 20 + (26 + 20\cdot(-1))\cdot(-3) = \\ = 20\cdot 4 + 26\cdot(-3) = \\ = (72 + 26\cdot(-2))\cdot 4 + 26\cdot(-3) = \\ = 72\cdot 4 + 26\cdot(-11). \end{gathered}$$

Таким образом, $2 = 72u + 26v$, где $u = 4$, $v = -11$.●

Замечание. Числа u и v не являются единственной парой с таким условием. Это следует из теории диофантовых линейных уравнений, которая будет рассмотрена ниже. Так, в примере 4 числа $u = -9$ и $v = 25$ также удовлетворяют соотношению Безу.

Следствие теоремы 4 (критерий взаимной простоты). Целые числа a и b взаимно просты тогда и только тогда, когда существуют такие целые u и v, что

$$au + bv = 1.$$

Доказательство. $\Rightarrow$) Если $(a,b) = 1$, то из соотношения Безу следует, что существуют такие целые числа u и v, что $au + bv = 1$.

$\Leftarrow$) Обратно, пусть существуют такие целые u и v, что $au + bv = 1$. Если $(a,b) = d > 1$, то $d \mid 1$ (по свойству делимости), а значит, $(a,b) = 1$. ◁

Расширенный алгоритм Евклида

При нахождении соотношения Безу более удобен ***расширенный*** (***обобщенный***) ***алгоритм Евклида***, позволяющий вычислять коэффициенты Безу параллельно с нахождением НОД.

Пусть $|a| > |b|$. Положим

$$\begin{aligned} u_0 &= 1, \quad v_0 = 0, \quad r_0 = a; \\ u_1 &= 0, \quad v_1 = 1, \quad r_1 = b. \end{aligned}$$

Далее последовательно вычисляем:

$$u_{i+1} = u_{i-1} - q_i u_i, \quad v_{i+1} = v_{i-1} - q_i v_i, \quad r_{i+1} = r_{i-1} - q_i r_i,$$

где q_i – неполное частное от деления r_{i-1} на r_i.

Работа алгоритма заканчивается, если на некотором шаге $r_{i+1} = 0$. При этом на предыдущем шаге найдены НОД и коэффициенты Безу:

$$(a,b) = r_i, \quad u = u_i, \quad v = v_i.$$

Обоснованием алгоритма служит следующая теорема.

Т 5. При всех *i* выполняется равенство: $u_i a + v_i b = r_i$.

Доказательство проводится индукцией по *i.*

1) *База индукции*: если $i = 0$ или $i = 1$, то, очевидно, равенство выполняется:

$$1 \cdot a + 0 \cdot b = a;$$
$$0 \cdot a + 1 \cdot b = b.$$

2) *Шаг индукции.* Предположим, что утверждение верно для всех $k \le i$. Тогда для следующего номера $i + 1$ получим

$$u_{i+1} \cdot a + v_{i+1} \cdot b = (u_{i-1} - q_i u_i) \cdot a + (v_{i-1} - q_i v_i) \cdot b =$$
$$= (u_{i-1} \cdot a + v_{i-1} \cdot b) - q_i \cdot (u_i \cdot a + v_i \cdot b) = r_{i-1} - q_i \cdot r_i = r_{i+1},$$

что и требовалось доказать. ◁

Пример 5. Найдем соотношение Безу для (72, 26) с помощью расширенного алгоритма Евклида.

Решение. Здесь $a = 72$, $b = 26$. Используем для оформления вычислений следующую таблицу. В столбцах *u*, *v*, *r* проводятся вычисления соответствующих величин. Первый столбец показывает схему всех вычислений. В столбце *q* записывается q_i – неполное частное от деления r_{i-1} на r_i, столбец *qb* бывает полезен при работе с большими числами.

	u	*v*	*r*	*q*	*qb*
a	1	0	72		
b	0	1	26	2	52
$a - qb$	1	–2	20	1	20
	–1	3	6	3	18
	4	–11	2	3	6
			0		

Работа алгоритма заканчивается, когда в столбце r появляется значение $r_{i+1} = 0$. Тогда в предыдущей строке получаем коэффициенты Безу $u = 4, v = -11$ и НОД(72,26) = 2. Таким образом, соотношение Безу для (72, 26) имеет вид $72 \cdot 4 + 26 \cdot (-11) = 2.\bullet$

Диофантовы линейные уравнения

Задача. Для газификации жилого дома требуется проложить газопровод протяженностью 150 м. Имеются трубы 13 и 9 м длиной. Возможно ли проложить газопровод, не разрезая трубы? Если да, то сколько труб каждого вида потребуется?

Эта задача приводит к уравнению

$$13x + 9y = 150$$

с целочисленными переменными x, y.

Опр. 5. ***Диофантовым линейным уравнением*** с двумя неизвестными называется уравнение вида

$$ax + by = c, \qquad (1)$$

где $a, b, c \in \mathbb{Z}$, $a, b \neq 0$, решения $(x; y)$ ищутся в целых числах. Иным словами, все коэффициенты и неизвестные – целые числа.

W W W В И К И С П Р А В К А W W W W W W W W W W W W W W W W W W W W W W

Диофа́нт Александри́йский
(др.-греч. Διόφαντος ὁ Ἀλεξανδρεύς;
лат. *Diophantus*)
(предположительно III в. н. э.)
древнегреческий математик; нередко упоминается как «отец алгебры».
Диофант был первым греческим математиком, который рассматривал дроби наравне с другими числами. Первым среди античных ученых предложил развитую математическую символику, которая позволяла формулировать полученные им результаты в достаточно компактном виде.
Автор «Арифметики» – книги, посвященной нахождению положительных рациональных решений неопределенных уравнений («диофантовых урав-

нений»). «Арифметика» Диофанта была утеряна после пожара в Александрийской библиотеке. Только в 1621 г. в Европе появился классический, подробно прокомментированный латинский перевод «Арифметики». При этом книга опережала уровень лучших алгебраических исследований XVI в.: в отличие от европейских алгебраистов того времени Диофант свободно оперировал отрицательными и рациональными числами, владел буквенной нотацией для уравнений, а самое главное – умел находить решения в целых и рациональных числах линейных, квадратных, кубических уравнений и систем с целыми коэффициентами с двумя и более неизвестными.

Т 6. Уравнение (1) разрешимо в целых числах тогда и только тогда, когда $(a,b)\vert c$.

Доказательство. 1) *Необходимость*. Пусть $(x_0;\, y_0)$ – целочисленное решение уравнения (1). Тогда справедливо равенство $ax_0+by_0=c$, а значит, по свойству делимости целых чисел $(a,b)\vert c$.

2) *Достаточность*. Пусть $d=(a,b)$ и $d\vert c$, тогда $c=dt$ для некоторого $t\in\mathbb{Z}$. Запишем соотношение Безу для $d=(a,b)$: существуют такие числа $u,v\in\mathbb{Z}$, что $au+bv=d$. Умножая последнее равенство на t, получаем $aut+bvt=c$, т. е. $(tu;\, tv)$ – целочисленное решение уравнения (1). $\triangleleft$

Т 7. Уравнение (1) либо не имеет решений в целых числах, либо имеет бесконечно много решений в целых числах.

Доказательство. Если $(a,b)\nmid c$, то в силу теоремы 6 уравнение (1) не имеет решений в целых числах.

Если $(a,b)\vert c$, то уравнение (1) разрешимо. При этом если $(x_0;\, y_0)$ – одно из решений уравнения (1), т. е. $ax_0+by_0=c$, то при произвольном целом t справедливо

$$a(x_0+bt)+b(y_0-at)=c,$$

а значит, $(x_0+bt;\, y_0-at)$ также является решением уравнения (1) при всех $t\in\mathbb{Z}$. $\triangleleft$

Можно показать, что имея одно решение $(x_0;\, y_0)$ уравнения (1), можно получить все его решения по формуле $\left(x_0+\frac{b}{d}t;\, y_0-\frac{a}{d}t\right)$, где $d=(a,b)$, $t\in\mathbb{Z}$. При этом частное решение

$(x_0; y_0)$ может быть найдено с помощью соотношения Безу для (a, b).

Алгоритм решения диофантова линейного уравнения (1).

1. Если $(a,b) \nmid c,$ то уравнение (1) не имеет решений в целых числах.

2. Если $(a, b) = d,\ d \mid c,$ то получаем (например, с помощью расширенного алгоритма Евклида) соотношение Безу для (a, b) и находим такие числа $u_0, v_0 \in \mathbb{Z},$ что

$$au_0 + bv_0 = d. \tag{2}$$

3. Умножив обе части равенства (2) на $\frac{c}{d},$ получим

$$a\frac{c}{d}u_0 + b\frac{c}{d}v_0 = c,$$

а значит, $x_0 = \frac{c}{d}u_0,\ y_0 = \frac{c}{d}v_0$ – частное решение уравнения (1).

4. Множество целочисленных решений уравнения (1) задается формулой

$$\left\{\left(x_0 + \frac{b}{d}t;\ y_0 - \frac{a}{d}t \right) \middle| \ t \in \mathbb{Z} \right\}. \tag{3}$$

Пример 6. Решим в целых числах уравнение $13x + 9y = 150$.

Решение. 1) Здесь a = 13, b = 9. Поскольку $a \neq 0, b \neq 0,$ найдем с помощью расширенного алгоритма Евклида НОД(13,9) и соотношение Безу для (13,9).

	u	v	r	q	qb
a	1	0	13	1	9
b	0	1	9	2	8
$a - qb$	1	–1	4	4	4
	–2	3	1		
			0		

Таким образом, в выделенной строке получаем коэффициенты Безу $u = -2, v = 3$ и НОД(13, 9) = 1, а соотношение Безу для (13, 9) имеет вид

$$13 \cdot (-2) + 9 \cdot 3 = 1.$$

2) Проверим условие $(a, b) \mid c$. Поскольку $d = (a, b) = 1$, $c = 150$ и $1 \mid 150$, умножим полученное соотношение Безу на $\frac{c}{d} = 150$:

$$13 \cdot (-300) + 9 \cdot 450 = 150.$$

Отсюда получаем частное решение исходного уравнения: $x_0 = -300, y_0 = 450$.

3) По формуле (3) находим все множество целочисленных решений исходного уравнения:

$$\{(-300 + 9t; 450 - 13t) : t \in \mathbb{Z}\}. \bullet$$

Полученное решение означает, в частности, что

$$13 \cdot (-291) + 9 \cdot 437 = 150;$$
$$13 \cdot (-210) + 9 \cdot 320 = 150;$$
$$13 \cdot (-30) + 9 \cdot 60 = 150;$$
$$13 \cdot 6 + 9 \cdot 8 = 150;$$
$$13 \cdot 15 + 9 \cdot (-5) = 150.$$

Таким образом, можно видеть, что в натуральных числах рассмотренное уравнение имеет единственное решение: $x = 6,\ y = 8$. Ответ на вопрос сформулированной выше задачи положительный: проложить газопровод, не разрезая трубы, возможно, если взять 6 труб длиной 13 м и 8 труб длиной 9 м.

Упражнение 2. Сколько существует способов составления отрезка длиной 1 м из отрезков длинами 7 и 12 см?

Многие старинные способы угадывания числа и месяца рождения основывались на умении решать диофантовы линейные уравнения. Например, чтобы угадать число и месяц рождения вашего собеседника, вам достаточно узнать у него сумму, получаемую от сложения двух произведений: даты дня рождения (x) на 12 и номера месяца (y) на 31. Причем из всех решений выбирается то единственное, для которого $1 \le x \le 31, 1 \le y \le 12$.

Упражнение 3. Определите число и месяц рождения человека, у которого вышеуказанная сумма равна 67.

§ 3. Сравнения. Классы вычетов

Т 1. Пусть m – натуральное число. Для любых целых чисел a и b следующие условия равносильны:

1) a и b имеют одинаковые остатки от деления на m;

2) $a-b$ делится на m, т. е. $a-b=mq$ для подходящего целого q;

3) $a=b+mq$ для некоторого целого q.

Доказательство проводится по схеме $1)\Rightarrow 2)\Rightarrow 3)\Rightarrow 1)$.

$1)\Rightarrow 2)$. Пусть $a=q_1m+r, b=q_2m+r,$ где $0\le r<m.$ Тогда $a-b=q_1m-q_2m=(q_1-q_2)m,$ т. е. $a-b$ делится на m.

$2)\Rightarrow 3)$. Если $a-b$ делится на m, т. е. $a-b=mq$ для некоторого $q\in\mathbb{Z},$ то $a=b+mq.$

$3)\Rightarrow 1)$. Пусть $a=q_1m+r_1, b=q_2m+r_2, 0\le r_1,r_2<m.$ Докажем, что если $a=b+mq,$ то $r_1=r_2$.

Подставляя в это соотношение выражения для a и b, получим $q_1m+r_1=q_2m+r_2+mq,$ откуда $r_1-r_2=(q_2+q-q_1)m,$ т. е. $m\,|\,r_1-r_2.$ Но поскольку $0\le r_1,r_2<m,$ то $r_1=r_2.\triangleleft$

Опр. 1. Целые числа a и b называются ***сравнимыми по модулю*** m, если они удовлетворяют одному из условий теоремы 1. Этот факт обозначают формулой $a\equiv b(\mathrm{mod}\,m)$.

Итак,

$$a\equiv b(\mathrm{mod}\,m) \quad\Leftrightarrow\quad \boxed{\begin{array}{c}a\text{ и }b\text{ имеют}\\ \text{одинаковые}\\ \text{остатки от де-}\\ \text{ления на }m\end{array}} \quad\Leftrightarrow\quad a-b\,\vdots\,m \quad\Leftrightarrow\quad \boxed{\begin{array}{c}a=b+mq\\ \text{для неко-}\\ \text{торого}\\ q\in\mathbb{Z}\end{array}}$$

Пример 1.

1) $7\equiv 11\equiv 23\equiv 3(\mathrm{mod}\,4);$

2) $-23\equiv 7(\mathrm{mod}\,10).\bullet$

Сравнения часто применяются для вычисления контрольных сумм, используемых в идентификаторах. Так, для определения ошибок при вводе международного номера банковского счета IBAN, состоящего из 34 символов, используется сравнение по модулю 97.

В химии последняя цифра в регистрационном номере химических соединений CAS является значением контрольной суммы, которая вычисляется путем сложения последней цифры номера, умноженной на 1, второй справа

цифры, умноженной на 2, третьей, умноженной на 3, и т. д. до первой слева цифры, завершаясь вычислением остатка от деления на 10.

Арифметические свойства сравнений

1. В сравнении можно отбрасывать или добавлять слагаемые, делящиеся на модуль: если $a \equiv b(\mathrm{mod}\, m)$, то для всякого $k \in \mathbb{Z}$

$$a \equiv (b \pm km)(\mathrm{mod}\, m).$$

2. Сравнения можно почленно складывать, вычитать, умножать, возводить в натуральную степень:

если $a \equiv b(\mathrm{mod}\, m)$, $c \equiv d(\mathrm{mod}\, m)$, то

$$(a \pm c) \equiv (b \pm d)(\mathrm{mod}\, m);$$

$$ac \equiv bd(\mathrm{mod}\, m);$$

$$a^n \equiv b^n(\mathrm{mod}\, m) \text{ при любом } n \in \mathbb{N}.$$

Доказательство. Докажем второе соотношение (сравнения можно почленно умножать). Если $a \equiv b(\mathrm{mod}\, m)$, $c \equiv d(\mathrm{mod}\, m)$, то $a = b + mq_1$, $c = d + mq_2$. Тогда

$$ac = (b + mq_1)(d + mq_2) = bd + mq_1 d + mq_2 b + m^2 q_1 q_2 = bd + mt, t \in \mathbb{Z}.$$

Следовательно, $ac \equiv bd(\mathrm{mod}\, m)$. ◁

Упражнение. Доказать первое соотношение.

3. К обеим частям сравнения можно прибавить или вычесть одно и то же число; обе части сравнения можно умножить на одно и то же число:

если $a \equiv b(\mathrm{mod}\, m)$, то для всякого $c \in \mathbb{Z}$

$$(a \pm c) \equiv (b \pm c)(\mathrm{mod}\, m);$$

$$ac \equiv bc(\mathrm{mod}\, m).$$

4. Сравнение можно сократить на общий множитель, взаимно простой с модулем: пусть $a = a_1 d$, $b = b_1 d$, $(d, m) = 1$, тогда

$$\text{если } a_1 d \equiv b_1 d(\mathrm{mod}\, m), \text{ то } a_1 \equiv b_1(\mathrm{mod}\, m).$$

Доказательство. Действительно,

$$a_1 d \equiv b_1 d(\mathrm{mod}\, m) \quad \Leftrightarrow \quad (a_1 d - b_1 d) \vdots m \quad \Leftrightarrow \quad d(a_1 - b_1) \vdots m,$$

откуда, поскольку d и m взаимно просты, следует $(a_1 - b_1) \vdots m$, т. е. $a_1 \equiv b_1 (\mathrm{mod}\, m)$. ◁

5. Если в сравнении $a \equiv b (\mathrm{mod}\, m)$ числа a, b, m имеют общий множитель d, то на него сравнение можно сократить:

$$\frac{a}{d} \equiv \frac{b}{d} \left(\mathrm{mod} \frac{m}{d} \right).$$

Доказательство. Сравнение $a \equiv b (\mathrm{mod}\, m)$ равносильно $a = b + mq$ при некотором $q \in \mathbb{Z}$. Тогда, так как числа a, b и m делятся на d, то $\frac{a}{d} = \frac{b}{d} + \frac{m}{d} q \Leftrightarrow \frac{a}{d} \equiv \frac{b}{d} \left(\mathrm{mod} \frac{m}{d} \right)$. ◁

6. $\begin{cases} a \equiv b (\mathrm{mod}\, m_1), \\ \quad ..., \\ a \equiv b (\mathrm{mod}\, m_k) \end{cases} \Leftrightarrow \quad a \equiv b (\mathrm{mod}[m_1, ..., m_k]).$

Доказательство. Сравнение $a \equiv b (\mathrm{mod}\, m_i)$ означает, что $(a - b) \vdots m_i$; указанная система сравнений означает, что число $a - b$ делится на каждое $m_i, 1 \le i \le k$, а значит $a - b$ делится на НОК чисел $m_i, 1 \le i \le k$, т. е. $(a - b) \vdots [m_1, ..., m_k] \Leftrightarrow a \equiv b (\mathrm{mod}[m_1, ..., m_k])$. ◁

7. Если $a \equiv b (\mathrm{mod}\, m)$, то $(a, m) = (b, m)$.

Доказательство. Сравнение $a \equiv b (\mathrm{mod}\, m)$ равносильно равенству $a = b + mq$ при некотором $q \in \mathbb{Z}$.

Тогда если $d \mid a$, $d \mid m$, то $d \mid b$; если $d \mid b$, $d \mid m$, то $d \mid a$, т. е. всякий делитель чисел a и m является делителем числа b, и всякий делитель чисел b и m является делителем числа a, а следовательно, $(a, m) = (b, m)$. ◁

Иногда полезно иметь в виду следующее утверждение, обобщающее и уточняющее свойства 3, 4 и 5.

Утв. 1.

1) При любом натуральном $c \neq 0$

$$a \equiv b (\mathrm{mod}\, m) \quad \Leftrightarrow \quad ac \equiv bc (\mathrm{mod}\, mc).$$

2) Если $(c, m) = 1$, то

$$a \equiv b (\mathrm{mod}\, m) \quad \Leftrightarrow \quad ac \equiv bc (\mathrm{mod}\, m).$$

Доказательство. **1)** По определению сравнения, $a \equiv b(\mathrm{mod}\, m)$ равносильно $a = b + mq$. При любом целом $c \neq 0$ это равенство равносильно $ac = bc + mqc$, т. е. $ac \equiv bc(\mathrm{mod}\, mc)$.

2) Второе утверждение объединяет свойства 3 и 4. $\triangleleft$

Отношение сравнимости как отношение эквивалентности

Пусть m – фиксированное натуральное число. Легко проверяются следующие три свойства:

1. *Рефлексивность*: $a \equiv a(\mathrm{mod}\, m)$ для любого целого a и всякого натурального m.

2. *Симметричность*: если $a \equiv b(\mathrm{mod}\, m)$, то $b \equiv a(\mathrm{mod}\, m)$.

3. *Транзитивность*: если $a \equiv b(\mathrm{mod}\, m)$, $b \equiv c(\mathrm{mod}\, m)$, то $a \equiv c(\mathrm{mod}\, m)$.

Данные свойства означают, что отношение сравнимости на множестве целых чисел $\mathbb{Z}$ есть ***отношение эквивалентности***. Это означает, что $\mathbb{Z}$ разбивается на непересекающиеся классы попарно сравнимых друг с другом по модулю m целых чисел.

Каждый класс сравнимых друг с другом целых чисел характеризуется общими свойствами представителей этого класса. Например, все они имеют один и тот же остаток от деления на модуль; все они в силу свойства 7 из арифметических свойств сравнений имеют одинаковый наибольший общий делитель с этим модулем и т. д.

Опр. 2. Множество всех чисел, сравнимых с a по модулю m, называется ***классом вычетов по модулю*** m (по-латински «residua» – «остаток, оставшаяся часть») и обозначается $\overline{a}$, т. е.

$$\overline{a} = \{b \in \mathbb{Z} : b \equiv a(\mathrm{mod}\, m)\},$$

или

$$\overline{a} = \{\ldots; a - 2m; a - m; a; a + m; a + 2m; \ldots\}.$$

Любое число из класса вычетов называют ***вычетом***. При обозначении класса вычетов можно использовать любой элемент класса, поскольку каждый представитель класса однозначно определяет свой класс, т. е. для любого числа $b \in \overline{a}$ класс $\overline{b} = \overline{a}$.

Утв. 2. $a \equiv b(\mathrm{mod}\, m) \Leftrightarrow \overline{a} = \overline{b}$.

Утв. 3. Различные классы вычетов не имеют общих элементов.

Множество классов вычетов

При делении целых чисел на натуральное число m существует ровно m различных остатков: $0, 1, ..., m-1$. Соответственно этим остаткам множество целых чисел $\mathbb{Z}$ разбивается на m непересекающихся классов вычетов по модулю m. В соответствии с остатком от деления на m эти классы обозначаются $\overline{0}, \overline{1}, ..., \overline{m-1}$.

Опр. 3. Множество всех классов сравнимых друг с другом чисел по модулю m называют ***множеством классов вычетов по модулю*** m и обозначают через $\mathbb{Z}/m\mathbb{Z}$ или $\mathbb{Z}_m$:

$$\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z} = \left\{\overline{0}; \overline{1}; ...; \overline{m-1}\right\}.$$

Таким образом, $\mathbb{Z}_m$ – множество из m элементов.

Пример 2. $\mathbb{Z}_7 = \mathbb{Z}/7\mathbb{Z} = \left\{\overline{0}; \overline{1}; \overline{2}; \overline{3}; \overline{4}; \overline{5}; \overline{6}\right\}.\bullet$

На множестве $\mathbb{Z}_m$ классов вычетов по заданному модулю можно ввести арифметические операции сложения, вычитания и умножения.

Опр. 4. ***Суммой*** классов вычетов $\overline{a}, \overline{b} \in \mathbb{Z}_m$ называется класс $\overline{a} + \overline{b} = \overline{a+b}$; ***разностью*** классов вычетов $\overline{a} \in \mathbb{Z}_m$ и $\overline{b} \in \mathbb{Z}_m$ называется класс $\overline{a} - \overline{b} = \overline{a-b}$; ***произведением*** классов вычетов $\overline{a}, \overline{b} \in \mathbb{Z}_m$ называется класс $\overline{a} \cdot \overline{b} = \overline{a \cdot b}$.

Таким образом, операции сложения, вычитания и умножения классов вычетов однозначно определяются соответствующими операциями над представителями этих классов. Как правило, сначала выполняют действие над обычными числами, а затем вычисляют остаток от деления результата на модуль m.

Пример 3. На множестве $\mathbb{Z}_7$

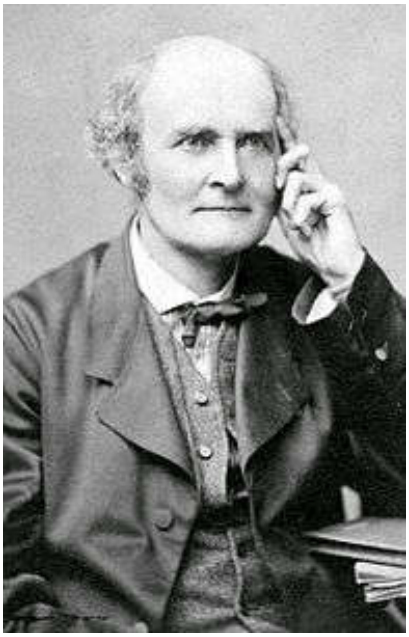
$$\overline{2} + \overline{5} = \overline{0}; \quad \overline{2} - \overline{5} = \overline{4}; \quad \overline{2} \cdot \overline{5} = \overline{3},$$

поскольку

$$2 + 5 = 7 \equiv 0 (\mathrm{mod}\, 7); \quad 2 - 5 = -3 \equiv 4 (\mathrm{mod}\, 7); \quad 2 \cdot 5 = 10 \equiv 3 (\mathrm{mod}\, 7).\bullet$$

Поскольку $\mathbb{Z}_m$ состоит из конечного множества элементов, то сложение и умножение удобно задавать поэлементно в виде таблиц. На пересечении i-й строки и j-го столбца таблицы пишется $x_i \circ x_j$ (где $\circ$ – знак операции). Такие таблицы называются ***таблицами Кэли***.

W W W В И К И С П Р А В К А W W W W W W W W W W W W W W W W W W W W W



А́ртур Кэ́ли
(англ. *Arthur Cayley*)
(1821–1895)
английский математик.
В детстве решал сложные математические задачи ради забавы. После окончания Кембриджского университета, где он был лучшим студентом курса, в течение 14 лет работал адвокатом, однако не переставал плодотворно заниматься математикой.
Один из самых плодовитых ученых XIX в., написавший более 700 работ. Большая часть его работ относится к линейной алгебре, дифференциальным уравнениям и эллиптическим функциям.
Таблицы Кэли использовались впервые в его статье 1854 г. в иллюстративных целях.

W W W W W W W W W W W W W W W W W W W W W W W W W W W W W W W W W W W

Пример 4. Построим таблицы сложения и умножения в $\mathbb{Z}_3$.

Множество $\mathbb{Z}_3$ классов вычетов по модулю 3 содержит 3 элемента:

$$\mathbb{Z}_3 = \mathbb{Z}/3\mathbb{Z} = \{\overline{0}; \overline{1}; \overline{2}\}.$$

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

$\times$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{1}$

Из таблицы умножения видно, что классы $\overline{1}$ и $\overline{2}$ обратны сами себе.●

Опр. 5. Элемент $\overline{a} \in \mathbb{Z}_m$ называется ***обратимым***, если найдется такой класс $\overline{b} \in \mathbb{Z}_m$, что $\overline{a} \cdot \overline{b} = \overline{1}$. В этом случае класс $\overline{b}$ называют ***обратным*** к классу $\overline{a}$.

Пример 5. Построим таблицы сложения и умножения в $\mathbb{Z}_6$.

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{5}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$

$\times$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{0}$	$\overline{2}$	$\overline{4}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{4}$	$\overline{2}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Из таблицы умножения видно, что обратимыми являются только классы $\overline{1}$ и $\overline{5}$, причем, как и в случае $\mathbb{Z}_3$, они обратны сами себе.●

Т 2. Класс $\overline{a} \in \mathbb{Z}_m$ обратим $\Leftrightarrow$ $(a, m) = 1$.

Полная и приведенная системы вычетов

Опр. 6. Любое множество представителей (по одному из каждого класса вычетов) называется ***полной системой вычетов по модулю*** m.

Пример 6. Примерами полной системы вычетов по модулю m будут, в частности: **1)** $0, 1, ..., m-1$; **2)** $1, 2, ..., m$. ●

Опр. 7. ***Приведенной системой вычетов по модулю*** m называется система чисел, взятых по одному из каждого класса, взаимно простого с m.

Пример 7. Составим приведенную систему вычетов по модулю 8.

Решение. Рассмотрим полную систему наименьших положительных вычетов по модулю 8: 1, 2, 3, 4, 5, 6, 7, 8.

Выбирая из этой системы только те вычеты, которые взаимно просты с модулем 8, получим приведенную систему вычетов:

1, 3, 5, 7.●

Из теоремы 2 можно сделать следующие несложные выводы.

Следствие 1. Множество обратимых классов образует приведенную систему вычетов.

Следствие 2. Если $m = p$ – простое число, то в $\mathbb{Z}_m$ каждый ненулевой класс обратим.

§ 4. Функция Эйлера. Теорема Эйлера. Малая теорема Ферма

Опр. 1. ***Функция Эйлера*** $\varphi(m)$ ставит в соответствие каждому натуральному $m > 1$ количество натуральных чисел, не превосходящих m и взаимно простых с m.

По определению полагается $\varphi(1) = 1$.

Пример 1. $\varphi(2) = 1$; $\varphi(3) = 2$; $\varphi(4) = 2$; $\varphi(5) = 4$; $\varphi(6) = 2$; $\varphi(7) = 6$.

Т 1 (о вычислении значений функции Эйлера).

1) $\varphi(p) = p - 1$ для каждого простого числа p;

2) $\varphi(p^s) = p^{s-1}(p-1)$, если p – простое число;

3) если $(m, n) = 1$, то $\varphi(mn) = \varphi(m)\varphi(n)$;

4) если $m = p_1^{s_1} p_2^{s_2} \dots p_t^{s_t}$ – каноническое разложение числа m, то

$$\boxed{\varphi(m) = p_1^{s_1-1}(p_1-1)p_2^{s_2-1}(p_2-1)\dots p_t^{s_t-1}(p_t-1).}$$

Доказательство. **1)** Количество чисел множества $\{1; 2; 3; \dots; p-1\}$, взаимно простых с p, равно $p-1$, так как любое число этого множества взаимно просто с p.

2) Разобьем множество чисел от 1 до p^s на последовательные группы по p элементов:

$$1; 2; 3; \dots; p-1; p;$$
$$p+1; p+2; p+3; \dots; 2p;$$
$$2p+1; 2p+2; 2p+3; \dots; 3p;$$
$$\dots;$$

$$(p^{s-1}-1)p+1;\ (p^{s-1}-1)p+2;\ (p^{s-1}-1)p+3;\ ...;\ p^s.$$

Здесь p^{s-1} строк, в каждой из них только одно последнее число делится на p, поэтому $\varphi(p^s)=p^s-p^{s-1}=p^{s-1}(p-1).$

3) Числа, взаимно простые с mn, взаимно просты с m и n одновременно. Чтобы определить количество чисел от 1 до mn, взаимно простых и с m, и с n, расположим натуральные числа от 1 до mn в виде следующей таблицы, содержащей m строк и n столбцов.

1	2	…	k	…	n
$n+1$	$n+2$	…	$n+k$	…	$2n$
…	…	…	…	…	…
$sn+1$	$sn+2$	…	$sn+k$	…	$(s+1)n$
…	…	…	…	…	…
$(m-1)n+1$	$(m-1)n+2$	…	$(m-1)n+k$	…	mn

В первой строке этой таблицы имеется ровно $\varphi(n)$ чисел, взаимно простых с n, причем некоторое число k из первой строки взаимно просто с n тогда и только тогда, когда и все числа k-го столбца также взаимно просты с n. Следовательно, таблица содержит $m\varphi(n)$ элементов, взаимно простых с n.

Отметим также, что числа k-го столбца (а их в каждом столбце ровно m) имеют попарно различные остатки от деления на m. Действительно, если предположить, что для различных целых $t,s,\ 0\le t<s\le m-1,$ числа $tn+k$ и $sn+k$ сравнимы по модулю m, то число $(sn+k)-(tn+k)=(s-t)n$ должно делиться на m, что невозможно, поскольку $(n, m) = 1$, а $0<s-t<m.$

Поэтому каждый столбец содержит столько же взаимно простых с m чисел, сколько их имеется среди всевозможных остатков от деления на m, т. е. $\varphi(m)$. Таким образом, в таблице содержится $\varphi(m)\varphi(n)$ чисел, взаимно простых и с m, и с n, а значит, $\varphi(mn)=\varphi(m)\varphi(n).$

4) Четвертое утверждение теоремы является следствием доказанных третьего и второго утверждений. ◁

Пример 2. Найдем $\varphi(48)$.

Решение. Поскольку $m=48=2^4\cdot 3,$ то

$$\varphi(48)=2^3\cdot(2-1)\cdot 3^0\cdot(3-1)=16.\bullet$$

Для доказательства теоремы Эйлера полезно обратить внимание на следующие два утверждения о приведенных системах вычетов.

Утв. 1. Любые $\varphi(m)$ чисел $x_1, x_2, ..., x_{\varphi(m)}$, попарно несравнимые по модулю m и взаимно простые с m, образуют приведенную систему вычетов по модулю m.

Утв. 2. Если $x_1, x_2, ..., x_{\varphi(m)}$ – приведенная система вычетов по модулю m, $(a,m)=1$, то числа $ax_1, ax_2, ..., ax_{\varphi(m)}$ также образуют приведенную систему вычетов по модулю m.

Доказательство. По свойству взаимно простых чисел, поскольку $(a,m)=1$, $(x_i,m)=1$, то $(ax_i,m)=1$. Таким образом, каждое из чисел $ax_1, ax_2, ..., ax_{\varphi(m)}$ взаимно просто с m.

Докажем теперь, что любые два числа из множества $ax_1, ax_2, ..., ax_{\varphi(m)}$ несравнимы по модулю m. Действительно, если бы было $ax_i \equiv ax_j \pmod m$, то, поскольку $(a,m)=1$, отсюда следовало бы $x_i \equiv x_j \pmod m$, что противоречит тому, что $x_1, x_2, ..., x_{\varphi(m)}$ – приведенная система вычетов.

Следовательно, имеем $\varphi(m)$ чисел, попарно несравнимых по модулю m и взаимно простых с m. В силу предыдущего утверждения они образуют приведенную систему вычетов по модулю m. $\triangleleft$

Т 2 [Эйлер, 1760]. Для $m \in \mathbb{N}, m>1, a \in \mathbb{Z}$

$$\boxed{(a,m)=1 \quad \Leftrightarrow \quad a^{\varphi(m)} \equiv 1 (\mathrm{mod}\, m).}$$

Доказательство. $\Rightarrow$) Пусть $x_1, x_2, ..., x_{\varphi(m)}$ – приведенная система вычетов по модулю m. В силу утверждения 2 при $(a,m)=1$ числа $ax_1, ax_2, ..., ax_{\varphi(m)}$ также образуют приведенную систему вычетов по модулю m. Установим взаимно однозначное соответствие между этими двумя системами, поставив каждому из чисел $ax_1, ax_2, ..., ax_{\varphi(m)}$ сравнимое с ним число из системы $x_1, x_2, ..., x_{\varphi(m)}$ так, что

$$ax_1 \equiv x_\alpha (\mathrm{mod}\, m),$$
$$ax_2 \equiv x_\beta (\mathrm{mod}\, m),$$
$$\ldots,$$

$$ax_{\varphi(m)} \equiv x_\nu (\mathrm{mod}\, m),$$

где $x_\alpha, x_\beta, ..., x_\nu$ – это некоторым образом переставленные числа $x_1, x_2, ..., x_{\varphi(m)}$.

Перемножив все эти сравнения, получим

$$a^{\varphi(m)} x_1 x_2 ... x_{\varphi(m)} \equiv x_\alpha x_\beta ... x_\nu (\mathrm{mod}\, m),$$

причем $x_\alpha x_\beta ... x_\nu = x_1 x_2 ... x_{\varphi(m)}$, поскольку это те же числа, некоторым образом переставленные. Поскольку каждое из чисел $x_1, x_2, ..., x_{\varphi(m)}$ взаимно просто с m, то и их произведение взаимно просто с m. Поэтому полученное сравнение можно сократить на произведение $x_1 x_2 ... x_{\varphi(m)} = x_\alpha x_\beta ... x_\nu$, что приводит к сравнению

$$a^{\varphi(m)} \equiv 1 (\mathrm{mod}\, m).$$

$\Leftarrow$) Поскольку $\varphi(m) \geq 1$, то из $a^{\varphi(m)} \equiv 1 (\mathrm{mod}\, m)$ следует, что $\bar{a} \cdot \overline{a^{\varphi(m)-1}} = \bar{1}$, а значит, $\bar{a}$ – обратимый элемент в $\mathbb{Z}_m$. Отсюда в силу теоремы 2 §3 заключаем, что $(a,m) = 1$. $\triangleleft$

Следствие (малая теорема Ферма). Если p – простое число, a – целое число, то

$$(a, p) = 1 \quad \Leftrightarrow \quad a^{p-1} \equiv 1 (\mathrm{mod}\, p).$$

Применения теоремы Эйлера

1. Нахождение обратных классов вычетов по данному модулю.

Как следует из доказательства теоремы Эйлера, если $\bar{a}$ – обратимый класс в $\mathbb{Z}_m$, то обратным к нему является класс

$$\bar{a}^{-1} = \overline{a^{\varphi(m)-1}}.$$

2. Нахождение остатка от деления на модуль больших степеней заданного числа.

Отметим, что возведение в степень с приведением по модулю является одной из важнейших операций теории чисел.

Пусть требуется найти $x \equiv a^b (\mathrm{mod}\, m)$ при $(a,m) = 1$. Тогда в силу свойств сравнений и теоремы Эйлера,

$$x \equiv a_1^{b_1} (\mathrm{mod}\, m), \text{ где } a \equiv a_1 (\mathrm{mod}\, m),\ b \equiv b_1 (\mathrm{mod}\, \varphi(m)).$$

(Попросту говоря, число a усекается до остатка от деления на m, а число b – до остатка от деления на $\varphi(m)$.)

Если $(a,m) = d > 1$ и $x \equiv a^b (\mathrm{mod}\, m)$, то $d \mid x$, поэтому, обозначив $a_1 = \frac{a}{d}, m_1 = \frac{m}{d}, x_1 = \frac{x}{d}$, получим

$$x_1 d \equiv a_1 d a^{b-1} (\mathrm{mod}\, m_1 d),$$

что равносильно

$$x_1 \equiv a_1 a^{b-1} (\mathrm{mod}\, m_1).$$

Пример 3. Найдем остаток от деления 171^{2147} на 52.

Решение. Пусть $x \equiv 171^{2147} (\mathrm{mod}\, 52)$.

1) Найдем НОД основания степени и модуля, т. е. (171, 52). Поскольку $171 = 9 \cdot 19 = 3^2 \cdot 19,\ 52 = 4 \cdot 13 = 2^2 \cdot 13,$ то (171, 52) = 1.

2) Упростим основание степени: $171 \equiv 15 (\mathrm{mod}\, 52)$.

3) Упростим показатель степени. Поскольку $52 = 4 \cdot 13 = 2^2 \cdot 13,$ то значение функции Эйлера $\varphi(52) = 2^1 \cdot (2-1) \cdot 13^0 \cdot (13-1) = 24.$ Так как $2147 \equiv 11 (\mathrm{mod}\, 24),$ то

$$x \equiv 15^{11} = \left(15^2\right)^5 \cdot 15 = \left(225\right)^5 \cdot 15 \equiv 17^5 \cdot 15 = \left(17^2\right)^2 \cdot 17 \cdot 15 (\mathrm{mod}\, 52);$$

$$x \equiv (289)^2 \cdot 17 \cdot 15 \equiv (29)^2 \cdot 17 \cdot 15 = 841 \cdot 17 \cdot 15 \equiv 9 \cdot 17 \cdot 15 (\mathrm{mod}\, 52);$$

$$x \equiv 51 \cdot 45 \equiv -1 \cdot (-7) = 7 (\mathrm{mod}\, 52).$$

Итак, остаток от деления 171^{2147} на 52 равен 7.●

Пример 4. Найдем остаток от деления 126^{1020} на 138.

Решение. Пусть $x \equiv 126^{1020} (\mathrm{mod} 138)$.

1) Найдем (126,138). Поскольку $126 = 6 \cdot 21 = 2 \cdot 3^2 \cdot 7,$ $138 = 2 \cdot 69 = 2 \cdot 3 \cdot 23,$ то (126,138) = 6.

Сравнение $x \equiv 126^{1020} (\mathrm{mod} 138)$ нужно сократить на 6. Пусть $x = 6x_1$. Тогда

$$x \equiv 126^{1020} (\mathrm{mod} 138) \quad \Leftrightarrow \quad 6x_1 \equiv 126 \cdot 126^{1020-1} (\mathrm{mod} 138);$$

$$6x_1 \equiv 6 \cdot 21 \cdot 126^{1019} (\mathrm{mod}\, 6 \cdot 23) \quad \Leftrightarrow \quad x_1 \equiv 21 \cdot 126^{1019} (\mathrm{mod}\, 23).$$

2) Упростим основание степени: $126 \equiv 11 (\mathrm{mod}\, 23)$.

3) Упростим показатель степени. Поскольку число 23 – простое, то $\varphi(23) = 23 - 1 = 22$. Так как $1019 \equiv 7 (\mathrm{mod}\, 22)$, то

$$x_1 \equiv 21 \cdot 11^7 \equiv -2 \cdot \left(11^2\right)^3 \cdot 11 = -22 \cdot (121)^3 \equiv 1 \cdot 6^3 (\mathrm{mod}\, 23);$$

$$x_1 \equiv 6^2 \cdot 6 \equiv 13 \cdot 6 = 78 \equiv 9 (\mathrm{mod}\, 23).$$

4) Следовательно, $x = 6x_1 = 54 (\mathrm{mod} 138)$.

Итак, остаток от деления 126^{1020} на 138 равен 54.●

§ 5. Решение линейных сравнений и их систем

Рассмотрим задачу решения линейного сравнения (сравнения 1-й степени)

$$ax \equiv b (\mathrm{mod}\, m) \qquad (1)$$

Задача решения таких сравнений используется, например, как часть процедуры, предназначенной для поиска ключей криптографической схемы RSA с открытым ключом.

Опр. 1. ***Решением сравнения*** (1) называется всякое целое число x_0, которое удовлетворяет этому сравнению.

Легко понять, что в этом случае вместе с числом x_0 сравнению удовлетворяют и все числа класса вычетов $\overline{x_0}$ по модулю m. Поэтому *класс вычетов по модулю m, числа которого удовлетворяют сравнению (1), считается за одно решение этого сравнения*. При таком соглашении сравнение (1) будет иметь столько решений, сколько классов вычетов по модулю m ему удовлетворяют. Поскольку полная система вычетов по модулю m состоит из m вычетов, то сравнение (1) может иметь только конечное количество решений или может не иметь их совсем.

Т 1. 1) Если $(a, m) = 1$, то сравнение (1) имеет единственное решение;

2) если $(a, m) = d > 1$ и $d \nmid b$, то сравнение (1) не имеет решений;

3) если $(a, m) = d > 1$ и $d \mid b$, то сравнение (1) имеет d решений.

Для доказательства первого утверждения теоремы отметим, что сравнение (1) равносильно диофантову уравнению

$$ax + my = b,$$

которое, согласно теореме 6 § 2, имеет решения тогда и только тогда, когда $d \mid b$, где $d = (a, m)$.

При этом множество всех решений диофантова уравнения описывается формулой $\left(x_0 + \frac{m}{d}t;\ y_0 - \frac{a}{d}t \right)$, где $(x_0; y_0)$ – частное решение этого уравнения, $d = (a, m)$, $t \in \mathbb{Z}$. Следовательно, решением сравнения (1) будет

$$x \equiv x_0 \left(\bmod \frac{m}{d} \right),$$

что равносильно совокупности d сравнений по модулю m:

$$\left[\begin{array}{l} x \equiv x_0 (\bmod m), \\ x \equiv x_0 + \frac{m}{d} (\bmod m), \\ \ldots, \\ x \equiv x_0 + (d-1)\frac{m}{d} (\bmod m). \end{array} \right.$$

Методы решения линейных сравнений

1. Метод перебора (подбора). При небольшом значении m сравнение $ax \equiv b (\bmod m)$ решается подбором.

При этом сравнение сокращают на $d = (a, m)$, а затем перебирают все классы вычетов по модулю m, подставляя их в сравнение.

2. Метод преобразования правой части сравнения путем добавления модуля. Сравнение сокращают на $d = (a, m)$, а для решения сравнения вида (1) с $d = (a, m) = 1$ рассматривают серию равносильных сравнений $ax \equiv b (\bmod m)$, $ax \equiv b + m (\bmod m)$, $ax \equiv b + 2m (\bmod m), \ldots, ax \equiv b + km (\bmod m), \ldots$, с целью получения в правой части числа $b + km$, делящегося на a, и сокращают.

Этот метод особенно целесообразен при небольших a, так как число испытываемых сравнений будет не больше, чем a.

Пример 1. Решим сравнение $3x \equiv 20 (\mathrm{mod} 161)$.

Решение. Здесь $a = 3$, $b = 20$, $m = 161$, причем $(3, 161) = 1$.

Так как $3 \nmid 20$, перейдем к равносильному сравнению, прибавив к правой части модуль:

$$3x \equiv 20 + 161 (\mathrm{mod} 161); \qquad 3x \equiv 181 (\mathrm{mod} 161).$$

Так как $3 \nmid 181$, прибавим модуль еще раз:

$$3x \equiv 181 + 161 (\mathrm{mod} 161); \qquad 3x \equiv 342 (\mathrm{mod} 161).$$

Сокращая сравнение на 3, получим $x \equiv 114 (\mathrm{mod} 161)$. ●

3. Использование расширенного алгоритма Евклида.

Пусть $(a, m) = d$ и $d \mid b$. Тогда, в силу свойств сравнений,

$$ax \equiv b (\mathrm{mod}\, m) \quad \Leftrightarrow \quad \frac{a}{d} x \equiv \frac{b}{d} \left(\mathrm{mod} \frac{m}{d} \right),$$

причем, как следует из теоремы 1, последнее сравнение имеет единственное решение по модулю $\frac{m}{d}$.

С помощью расширенного алгоритма Евклида можно получить соотношение Безу для $(a, m) = d$ или $\left(\frac{a}{d}, \frac{m}{d} \right) = 1$ (коэффициенты Безу совпадают):

$$au_0 + mv_0 = d \quad \Leftrightarrow \quad \frac{a}{d} u_0 + \frac{m}{d} v_0 = 1.$$

Умножая последнее соотношение на b, получим

$$\frac{a}{d} bu_0 + \frac{m}{d} bv_0 = b \quad \Leftrightarrow \quad a \frac{b}{d} u_0 \equiv b \left(\mathrm{mod} \frac{m}{d} \right),$$

а значит, решением преобразованного, а следовательно, и исходного сравнения является

$$\boxed{x \equiv \frac{b}{d} u_0 \left(\mathrm{mod} \frac{m}{d} \right).}$$

Пример 2. Решим сравнение $15x \equiv 39 (\mathrm{mod} 84)$.

Решение. 1) Здесь a = 15, b = 39, m =84. Найдем с помощью расширенного алгоритма Евклида НОД$(15,84)$ и соотношение Безу для $(15,84)$.

	u	v	r	q	qb
a	1	0	84		
b	0	1	15	5	75
$a-qb$	1	–5	9	1	9
	–1	6	6	1	6
	2	–11	3	2	6
			0		

Таким образом, в выделенной строке получаем коэффициенты Безу $u_0 = 2, v_0 = -11$ и НОД$(15, 84)$ = 3, а соотношение Безу для $(15, 84)$ имеет вид

$$84 \cdot 2 + 15 \cdot (-11) = 3.$$

Следовательно, $15 \cdot (-11) \equiv 3 (\mathrm{mod}\, 84)$.

2) Поскольку $d = (a,m)$ = 3, $b = 39$ и $3 \mid 39$, то решением исходного сравнения будет

$$x \equiv \frac{39}{3} \cdot (-11) \left(\mathrm{mod}\, \frac{84}{3} \right);$$

$$x \equiv -143 \left(\mathrm{mod}\, 28 \right).$$

Упрощая, получим $x \equiv -3 \left(\mathrm{mod}\, 28 \right)$. •

Замечание. Сравнение всегда можно упростить, разделив обе части сравнения и модуль на их общий делитель:

$$ax \equiv b (\mathrm{mod}\, m) \quad \Leftrightarrow \quad \frac{a}{d} x \equiv \frac{b}{d} \left(\mathrm{mod}\, \frac{m}{d} \right).$$

4. Применение теоремы Эйлера. Пусть задано сравнение

$$ax \equiv b (\mathrm{mod}\, m), \text{ где } (a,m) = 1.$$

По теореме Эйлера $a^{\varphi(m)} \equiv 1 (\mathrm{mod}\, m)$, откуда $a^{\varphi(m)} b \equiv b (\mathrm{mod}\, m)$, или $a \cdot a^{\varphi(m)-1} b \equiv b (\mathrm{mod}\, m)$. Следовательно, решением исходного сравнения будет

$$x \equiv a^{\varphi(m)-1} b (\mathrm{mod}\, m).$$

Если $(a,m) = d > 1$, исходное сравнение нужно сократить на *d.*

Пример 3. Решим сравнение $7x \equiv 5(\mathrm{mod}\, 9)$.

Решение. Поскольку (7,9) = 1, решим сравнение с помощью теоремы Эйлера. Так как $9 = 3^2$, то значение функции Эйлера $\varphi(9) = 3^1 \cdot (3-1) = 6$. Решение исходного сравнения можно найти по формуле

$$x \equiv 7^{\varphi(9)-1} \cdot 5(\mathrm{mod}\, 9);$$

$$x \equiv 7^5 \cdot 5(\mathrm{mod}\, 9).$$

Поскольку $7 \equiv -2(\mathrm{mod}\, 9)$, то $7^5 \equiv (-2)^5 = -32 \equiv 4(\mathrm{mod}\, 9)$, а значит,

$$x \equiv 4 \cdot 5 = 20 \equiv 2(\mathrm{mod}\, 9).$$

Итак, $x \equiv 2(\mathrm{mod}\, 9)$. •

Замечание. Отметим, что метод решения сравнения, основанный на применении теоремы Эйлера, нельзя отнести к рациональным методам решения сравнений

Система сравнений первой степени

Т 2 (китайская теорема об остатках). Пусть $m_1, m_2, ..., m_k$ – *попарно взаимно простые* натуральные числа, а $c_1, c_2, ..., c_k$ – целые числа. Тогда множество решений системы сравнений

$$\begin{cases} x \equiv c_1 (\mathrm{mod}\, m_1), \\ \quad ..., \\ x \equiv c_k (\mathrm{mod}\, m_k) \end{cases}$$

имеет вид

$$\boxed{x \equiv c_1 x_1 \frac{m}{m_1} + ... + c_k x_k \frac{m}{m_k} (\mathrm{mod}\, m),}$$

где $m = [m_1, m_2, ..., m_k]$, x_i – произвольное целое число, удовлетворяющее сравнению $\boxed{x_i \frac{m}{m_i} \equiv 1 (\mathrm{mod}\ m_i).}$

По существу, эта теорема утверждает, что можно восстановить целое число по множеству его остатков от деления на числа из некоторого набора попарно взаимно простых чисел.

На практике китайская теорема об остатках позволяет работать не с длинными числами, а с наборами их коротких по длине остатков, поскольку устанавливает взаимно однозначное соответствие между числом и множеством его остатков, определяемым набором взаимно простых чисел. Если в качестве базиса взять, к примеру, первые 500 простых чисел, длина каждого из которых не превосходит 12 бит, то этого хватит для представления десятичных чисел длиной до 1500 знаков.

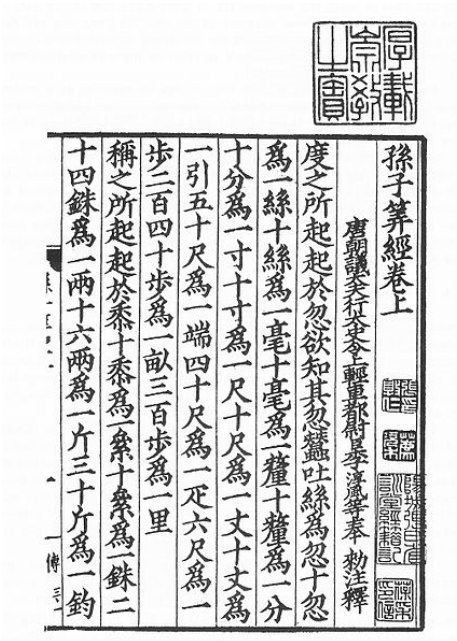
Кроме того, вычисления по каждому из модулей можно выполнять параллельно.

WWW ВИКИСПРАВКА WWWWWWWWWWWWWWWWWWWWWW

Эта теорема в ее арифметической формулировке была описана в трактате китайского математика Сунь Цзы «Сунь Цзы Суань Цзин» («Математическое наставление Сунь Цзы», предположительно III в. н. э.) и затем обобщена Цинь Цзю-шао в его книге «Математические рассуждения в 9 главах» (1247).

Сунь Цзы
(кит. трад. 孫子, упр. 孙子,
пиньинь: *sūn zǐ*)
(приблизительно III в. н. э.)
китайский математик и астроном, автор трактата «Сунь Цзы Суань Цзин» («Математическое наставление Сунь Цзы»). Занимаясь разработкой календаря, он открыл утверждение, известное как китайская теорема об остатках.

Цинь Цзю-шао
(кит. 秦九韶)
(XIII в.)
китайский математик. Считается одним из великих алгебраистов XIII–XIV вв. Автор сочинения «Математические рассуждения в 9 главах», в котором впервые в китайской литературе использован


孫子算經卷上

度之所起起於忽欲知其忽蠶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黍十黍爲一累十累爲一銖二十四銖爲一兩十六兩爲一斤三十斤爲一鈞

символ для нуля в виде кружка. Сочинение посвящено теории чисел и решению алгебраических уравнений.

Пример 3. Решим систему сравнений $\begin{cases} 7x \equiv 11 (\mathrm{mod}\, 18), \\ 8x \equiv 1 (\mathrm{mod}\, 27), \\ 9x \equiv 13 (\mathrm{mod}\, 28). \end{cases}$

Решение. 1) Разложим каждый из модулей на взаимно простые множители и в силу свойства 6 из арифметических свойств сравнений заменим каждое сравнение равносильной системой сравнений:

$$\begin{cases} 7x \equiv 11 (\mathrm{mod}\, 2),\ 7x \equiv 11 (\mathrm{mod}\, 9), \\ \qquad\qquad 8x \equiv 1 (\mathrm{mod}\, 27), \\ 9x \equiv 13 (\mathrm{mod}\, 4),\ 9x \equiv 13 (\mathrm{mod}\, 7). \end{cases}$$

2) Решим каждое из сравнений.

Поскольку $7 \equiv 1 (\mathrm{mod}\, 2)$ и $11 \equiv 1 (\mathrm{mod}\, 2)$, то сравнение $7x \equiv 11 (\mathrm{mod}\, 2)$ равносильно $x \equiv 1 (\mathrm{mod}\, 2)$.

Поскольку $7 \equiv -2 (\mathrm{mod}\, 9)$ и $11 \equiv 2 (\mathrm{mod}\, 9)$, то упрощение сравнения $7x \equiv 11 (\mathrm{mod}\, 9)$ приводит к сравнению $-2x \equiv 2 (\mathrm{mod}\, 9)$, откуда, очевидно, $x \equiv -1 (\mathrm{mod}\, 9)$, или $x \equiv 8 (\mathrm{mod}\, 9)$.

Сравнение $8x \equiv 1 (\mathrm{mod}\, 27)$ решим с помощью расширенного алгоритма Евклида:

	u	v	r		
a	1	0	27	q	qb
b	0	1	8	3	24
$a-qb$	1	–3	3	2	6
	–2	7	2	1	2
	3	–10	1	2	2
			0		

Таким образом, в выделенной строке получаем коэффициенты Безу $u_0 = 3, v_0 = -10$ для НОД$(27, 8) = 1$, а соотношение Безу для $(27, 8)$ имеет вид

$$27 \cdot 3 + 8 \cdot (-10) = 1.$$

Следовательно, $8 \cdot (-10) \equiv 1 (\mathrm{mod}\, 27)$, т. е. $x \equiv -10 (\mathrm{mod}\, 27)$, или $x \equiv 17 (\mathrm{mod}\, 27)$.

Упрощая следующее сравнение $9x \equiv 13 (\mathrm{mod}\, 4)$, получим $x \equiv 1 (\mathrm{mod}\, 4)$.

Упрощение сравнения $9x \equiv 13 (\mathrm{mod}\, 7)$ приводит к сравнению $2x \equiv 6 (\mathrm{mod}\, 7)$, откуда, очевидно, $x \equiv 3 (\mathrm{mod}\, 7)$.

Таким образом, исходная система сравнений равносильна системе

$$\begin{cases} x \equiv 1 (\mathrm{mod}\, 2), x \equiv 8 (\mathrm{mod}\, 9), \\ \quad x \equiv 17 (\mathrm{mod}\, 27), \\ x \equiv 1 (\mathrm{mod}\, 4), x \equiv 3 (\mathrm{mod}\, 7). \end{cases}$$

3) Упростим систему сравнений так, чтобы остались только взаимно простые модули.

Сравнение $x \equiv 1 (\mathrm{mod}\, 2)$ равносильно совокупности сравнений $\left[\begin{array}{l} x \equiv 1 (\mathrm{mod}\, 4), \\ x \equiv 3 (\mathrm{mod}\, 4), \end{array}\right.$ поэтому система сравнений $\begin{cases} x \equiv 1 (\mathrm{mod}\, 2), \\ x \equiv 1 (\mathrm{mod}\, 4) \end{cases}$ равносильна сравнению $x \equiv 1 (\mathrm{mod}\, 4)$.

Поскольку сравнение $x \equiv 8(\mathrm{mod}\,9)$ равносильно совокупности сравнений $\left[\begin{array}{l} x \equiv 8(\mathrm{mod}\,27), \\ x \equiv 17(\mathrm{mod}\,27), \\ x \equiv 26(\mathrm{mod}\,27), \end{array}\right.$ то система сравнений $\begin{cases} x \equiv 8(\mathrm{mod}\,9), \\ x \equiv 17(\mathrm{mod}\,27) \end{cases}$ равносильна сравнению $x \equiv 17\left(\mathrm{mod}\,27\right)$.

Следовательно, исходная система сравнений равносильна системе

$$\begin{cases} x \equiv 1(\mathrm{mod}\,4), \\ x \equiv 17(\mathrm{mod}\,27), \\ x \equiv 3(\mathrm{mod}\,7). \end{cases}$$

4) К последней системе применим китайскую теорему об остатках. Здесь $c_1 = 1, c_2 = 17, c_3 = 3,$ модули $m_1 = 4, m_2 = 27, m_3 = 7$ – попарно взаимно простые натуральные числа, их НОК равно $m = 4 \cdot 27 \cdot 7 = 756.$ Решение системы сравнений находится по формуле

$$x \equiv c_1 x_1 \frac{m}{m_1} + c_2 x_2 \frac{m}{m_2} + c_3 x_3 \frac{m}{m_3} \left(\mathrm{mod}\ m\right),$$

где x_1, x_2, x_3 – произвольные целые числа, удовлетворяющие системе сравнений

$$\begin{cases} \dfrac{756}{4} x_1 \equiv 1(\mathrm{mod}\,4), \\ \dfrac{756}{27} x_2 \equiv 1(\mathrm{mod}\,27), \\ \dfrac{756}{7} x_3 \equiv 1(\mathrm{mod}\,7) \end{cases} \Leftrightarrow \begin{cases} 189 x_1 \equiv 1(\mathrm{mod}\,4), \\ 28 x_2 \equiv 1(\mathrm{mod}\,27), \\ 108 x_3 \equiv 1(\mathrm{mod}\,7). \end{cases}$$

Упрощая каждое из сравнений, поскольку $189 \equiv 1(\mathrm{mod}\,4),$ $28 \equiv 1(\mathrm{mod}\,27),$ $108 \equiv 3(\mathrm{mod}\,7),$ получим

$$\begin{cases} x_1 \equiv 1(\mathrm{mod}\,4), \\ x_2 \equiv 1(\mathrm{mod}\,27), \\ 3x_3 \equiv 1(\mathrm{mod}\,7), \end{cases} \Leftrightarrow \begin{cases} x_1 \equiv 1(\mathrm{mod}\,4), \\ x_2 \equiv 1(\mathrm{mod}\,27), \\ x_3 \equiv 5(\mathrm{mod}\,7). \end{cases}$$

Таким образом, $x_1 = 1, x_2 = 1, x_3 = 5$. Следовательно, решение исходной системы сравнений имеет вид

$$x \equiv 1 \cdot 1 \cdot 189 + 17 \cdot 1 \cdot 28 + 3 \cdot 5 \cdot 108 (\mathrm{mod}\ 756),$$

т. е. $x \equiv 2285 (\mathrm{mod}\ 756)$, или $x \equiv 17 (\mathrm{mod}\ 756)$. ●

§ 6. Применение в криптографии

Криптография (др.-греч. κρυπτός «скрытый» + γράφω «пишу») – наука о методах обеспечения конфиденциальности (невозможности прочтения информации посторонним), целостности данных (невозможности незаметного изменения информации), аутентификации (проверки подлинности авторства или иных свойств объекта), а также невозможности отказа от авторства.

Современный период развития криптографии (с конца 1970-х гг.) связан с зарождением и развитием нового направления – ***криптографии с открытым ключом***, или ***асимметричной криптографии***, в которой алгоритм шифрования и открытый ключ являются общедоступными, а закрытый ключ известен только получателю. Суть шифрования с открытым ключом заключается в том, что для шифрования данных используется один ключ (открытый), а для расшифровывания – другой (закрытый).

По современным оценкам, около 10 млрд устройств в мире используют шифрование с открытым ключом.

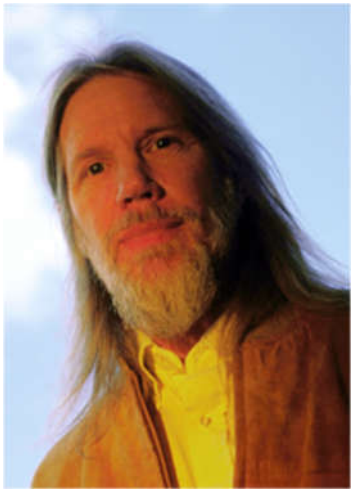
Надежность шифрования базируется на исключительной трудности задачи определения закрытого ключа на основании открытого. В основе каждой из известных асимметричных криптосистем лежит одна из сложных математических проблем в области ***теории чисел*** или ***алгебры***.

Алгоритм Диффи – Хеллмана

Основы криптографии с открытым ключом были выдвинуты У. Диффи и М. Хеллманом в 1976 г. в статье «Новые направления в криптографии», в которой авторы под влиянием работ Р. Меркла описали способ получения секретных ключей через открытый канал. Предложенный метод генерации ключей основан на возведении в степень на множестве классов вычетов по модулю либо в конечном поле.

В статье У. Диффи и М. Хеллмана был представлен радикально новый подход к распределению криптографических ключей, основанный на идее о том, что ключи можно использовать парами – ключ зашифрования и ключ расшифрования – при условии, что исключается возможность определения содержимого ключа для расшифрования исходя из содержимого открыто передаваемого ключа для зашифрования. Тем самым в криптографии нашлось решение одной из фундаментальных проблем – проблемы распределения ключей.

W W W В И К И С П Р А В К А W W W W W W W W W W W W W W W W W W W W W W W W W



Уитфилд Диффи

(англ. *Bailey Whitfield 'Whit' Diffie)*

(род. 1944)

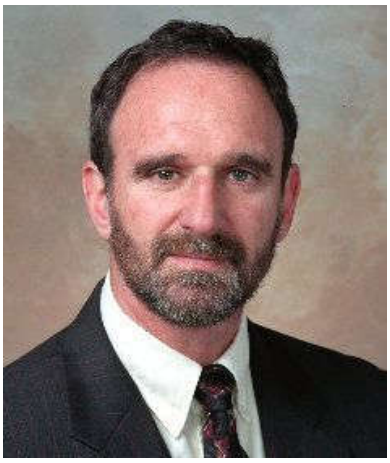
один из самых известных американских криптографов, заслуживший мировую известность за концепцию криптографии с открытым ключом.

Он одним из первых предсказал революцию в области информационных технологий, заявив, что, учитывая темпы роста мощностей и уменьшение размеров вычислительных систем, в скором времени компьютеры станут доступны всем желающим.

Включившись в Стэнфордском университете в работу над проектом ARPANet, он также предвидел создание интернета. Эти предсказания были одной из причин, по которой Диффи всерьез занялся проблемой распределения ключей. Он был убежден, что если люди будут обмениваться информацией с помощью компьютеров, они должны иметь право на приватность и быть способными зашифровывать необходимую информацию.

W W W W W W W W W W W W W W W W W W W W W W W W W W W W W W W W W W W W W W W

W W W В И К И С П Р А В К А W W W W W W W W W W W W W W W W W W W W W W W W W



Ма́ртин Хе́ллман
(англ. *Martin E. Hellman*)
(род. 1945)
американский криптограф. Получил известность благодаря разработке первой асимметричной криптосистемы в соавторстве с У. Диффи и Р. Мерклем в 1976 г. Еще тогда предвидел, что электронные переводы денежных средств из одного банка в другой повлекут за собой огромную проблему шифрования данных.

W W W W W W W W W W W W W W W W W W W W W W W W W W W W W W W W W W

W W W В И К И С П Р А В К А W W W W W W W W W W W W W W W W W W W W

Ральф Чарльз Меркл
(англ. *Ralph Charles Merkle*)
(род. 1952)
американский криптограф, известный своими работами в области криптосистем с открытым ключом (протокол Диффи – Хеллмана – Меркла) и хеширования (структура Меркла – Дамгарда).

W W W W W W W W W W W W W W W W W W W W W W W W W W W W W W W W W W

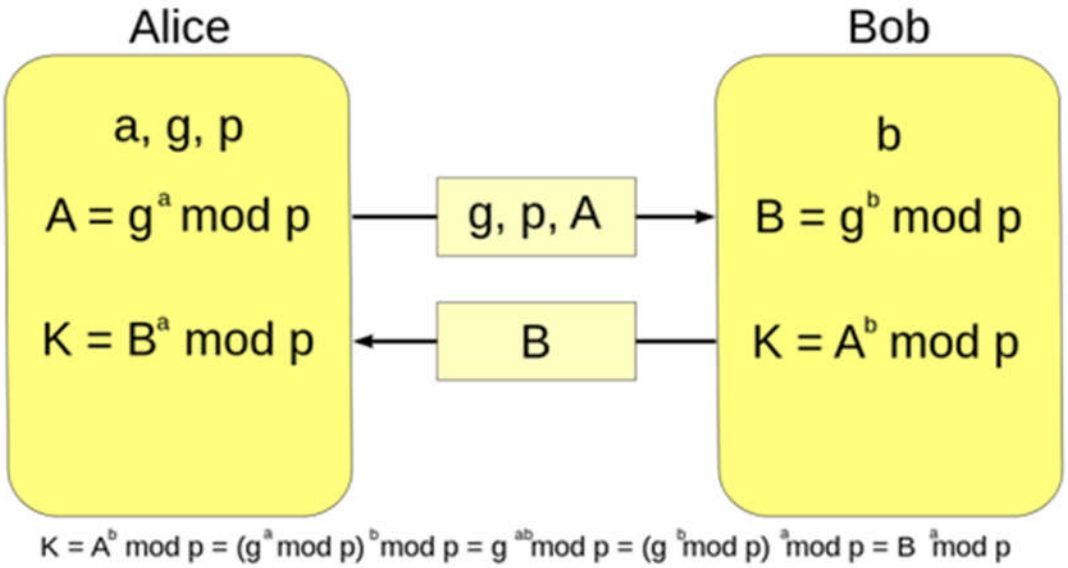
Алгоритм Диффи – Хеллмана создания секретного ключа заключается в следующем.

Пусть два пользователя (Алиса и Боб) хотят согласовать ключ – класс вычетов по модулю $m = p$ (p – простое число), с помощью которого они планируют шифровать свою переписку. При этом значение p общеизвестно; фиксируется и также не является секретным число g (в идеале, хотя и не обязательно, g – *первообразный корень* по модулю p).

На первом этапе каждая сторона выбирает некоторое число между 1 и $p - 1$, возводит g в выбранную степень (по модулю p) и посылает результат партнеру: Алиса выбирает свой закрытый ключ – число $a, 1 < a < p - 1,$ и посылает Бобу свой открытый ключ $A \equiv g^a \pmod{p}$; Боб выбирает свой закрытый ключ – число

$b, 1 < b < p-1,$ и отправляет Алисе свой *открытый ключ* $B \equiv g^b \pmod p$.

На втором этапе каждый из участников возводит полученный открытый ключ партнера в степень, равную своему закрытому ключу, и получает *общий секретный ключ*, поскольку $K \equiv B^a \equiv g^{ab} \pmod p$ и $K \equiv A^b \equiv g^{ab} \pmod p$ представляют один и тот же класс вычетов из множества $\mathbb{Z}_p$.



Таким образом, алгоритм Диффи – Хеллмана позволяет двум сторонам получить общий секретный ключ, используя незащищенный от прослушивания, но защищенный от подмены канал связи. Поскольку криптосистемы с открытым ключом значительно медленнее классических криптосистем, то они используются для генерации общего секретного ключа, который затем используется при обмене сообщениями с помощью классических симметричных криптосистем.

Безопасность криптосистемы Диффи – Хеллмана обеспечивается трудноразрешимостью *задачи дискретного логарифмирования* – задачи восстановления показателя степени в классах вычетов по известному результату при данных основании степени и модуле. В настоящее время не существует алгоритма, решающего эту задачу с полиномиальной сложностью.

Замечание. В практических реализациях для повышения стойкости криптосистемы в качестве a и b используются числа порядка 10^{100}, а p – порядка 10^{300}. Число g не обязано быть большим и обычно имеет значение в пределах первого десятка.

В 2015 г. У. Диффи и М. Хеллман были награждены премией Тьюринга «за фундаментальный вклад в криптографию».

W W W В И К И С П Р А В К А W W W W W W W W W W W W W W W W W W

Премия Тьюринга (англ. *Turing Award*) — самая престижная премия в информатике, вручаемая Ассоциацией вычислительной техники за выдающийся научно-технический вклад в этой области. Вручается ежегодно одному или нескольким специалистам в области информатики и вычислительной техники, чей вклад оказал сильное и продолжительное влияние на компьютерное сообщество. Премия может быть присуждена одному человеку не более одного раза.

В сфере информационных технологий премия Тьюринга имеет статус, аналогичный Нобелевской премии в академических науках.

W W W W W W W W W W W W W W W W W W W W W W W W W W W W W W W

Понятие о проблеме дискретного логарифмирования

Задача дискретного логарифмирования – это задача решения сравнения $g^x \equiv a \pmod{m}$ при заданных a, m и g.

Задача дискретного логарифмирования может быть легко решена, если модуль m не очень велик.

В общем случае эффективные методы решения задачи дискретного логарифмирования неизвестны. Полиномиального алгоритма для решения этой задачи пока не существует.

По вычислительной сложности алгоритмы решения задачи дискретного логарифмирования в поле вычетов разделяют на экспоненциальные и субэкспоненциальные.

Алгоритмы экспоненциальной сложности:

– алгоритм согласования;

– алгоритм Гельфонда – Шенкса (алгоритм больших и малых шагов, baby-step giant-step, А. Гельфонд, 1962, D. Shanks, 1972);

– алгоритм Силвера – Полига – Хеллмана (R. Silver, S. Pohlig, M. Hellman, 1978) – применяется, если известно разложение числа $p-1$ на простые множители; эффективен в случае, если множители, на которые раскладывается число $p-1$, достаточно малы;

– ρ-метод Полларда (J. M. Pollard, 1978) – не дает выигрыша по времени, но требует малое количество памяти.

Алгоритмы субэкспоненциальной сложности:

– алгоритм Адлемана (L. M. Adleman, 1979) – первый субэкспоненциальный алгоритм дискретного логарифмирования, но на практике он недостаточно эффективен;

– алгоритм COS – алгоритм Копперсмита – Одлыжко –Шреппеля (D. Coppersmith, A. Odlyzko, R. Schroeppel, 1986);

– метод решета числового поля (Number Field Sieve NFS, предложен для факторизации целых чисел (J. M. Pollard, 1988), а затем перенесен на задачу дискретного логарифмирования (D. Gordon, 1993), позднее было предложено множество различных улучшений данного алгоритма).

W W W В И К И С П Р А В К А W W W W W W W W W W W W W W W W W W W W

Экспериментально показано, что при $p \le 10^{90}$ алгоритм COS лучше решета числового поля, а при $p > 10^{100}$ решето числового поля быстрее, чем COS.

На данный момент самым мощным методом решения задачи дискретного логарифмирования считается метод решета числового поля.

Современные рекорды в дискретном логарифмировании получены именно с помощью метода решета числового поля: в декабре 2019 г. был установлен новый рекорд по вычислению дискретных логарифмов по модулю 240-значного *безопасного простого числа*; предыдущий рекорд был поставлен в июне 2016 г. – по модулю 232-значного *безопасного простого числа*; до этого – в июне 2014 г. по модулю 180-значного *безопасного простого числа*; в феврале 2007 г. по модулю 160-значного *безопасного простого числа*.

Безопасное простое число – это простое число вида $2p+1,$ где p также простое.

Безопасные простые числа используются в криптографических алгоритмах, основанных на дискретных логарифмах, поскольку их использование повышает стойкость криптосистемы против атаки с помощью алгоритма Силвера – Полига – Хеллмана.

W W W W W W W W W W W W W W W W W W W W W W W W W W W W W W W W W W

Современные алгоритмы вычисления дискретного логарифма имеют очень высокую сложность, которая сравнима со сложностью наиболее быстрых алгоритмов разложения чисел на множители. В связи с этим задача дискретного логарифмирования является одной из основных задач, на которых базируется криптография с открытым ключом.

Вычислительная сложность решения этой задачи составляет основу целого ряда алгоритмов криптографии:

– криптосистемы с открытым ключом по Диффи – Хеллману (W. Diffie, M. E. Hellman, 1976);

– криптосистемы и схемы электронной цифровой подписи Эль-Гамаля (T. ElGamal, 1984);

– криптосистемы Мэсси – Омуры для передачи сообщений (J. L. Massey, J. K. Omura, 1986)

– DSA-алгоритма цифровой подписи (Digital Signature Algorithm, 1991).

Криптосистема RSA

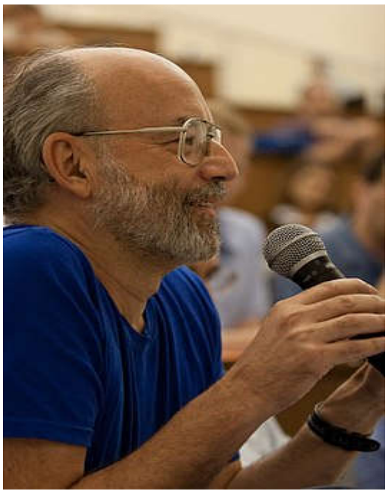
В 1977 г. был изобретен первый алгоритм асимметричного шифрования RSA, который позволил решить проблему общения через незащищенный канал. Метод RSA назван по первым буквам фамилий его создателей Р. Ривеста, А. Шамира, Л. Адлемана и основан на трудноразрешимости *задачи факторизации больших целых чисел*, т. е. на различии в том, насколько легко находить большие простые числа и насколько сложно раскладывать на множители произведение двух больших простых чисел. Сложность наиболее быстрых алгоритмов факторизации целых чисел сравнима со сложностью решения задачи дискретного логарифмирования.

W W W В И К И С П Р А В К А W W W W W W W W W W W W W W W W W W W W

Ро́нальд Линн Ривест
(англ. *Ronald Linn Rivest)*
(род. 1947)
американский специалист по криптографии. Является соавтором учебника «Алгоритмы: построение и анализ» (совместно с Т. Корменом, Ч. Лейзерсоном и К. Штайном), который считается фундаментальным трудом в области алгоритмов.

W W W W W W W W W W W W W W W W W W W W W W W W W W W W W W W W W W

W W W В И К И С П Р А В К А W W W W W W W W W W W W W W W W W W W W



Ади Шамир
(ивр. עדי שמיר)
(род. 1952)

известный израильский криптоаналитик, ученый в области теории вычислительных систем.

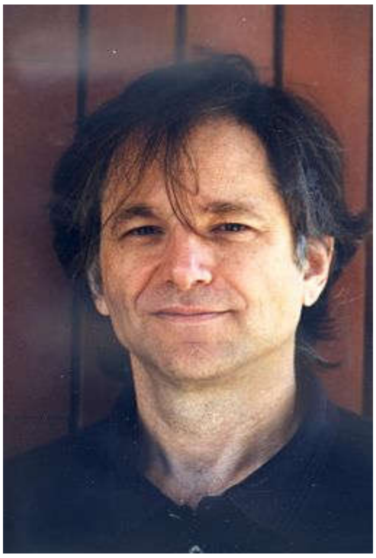
А. Шамира называют криптографическим «гуру» и «патриархом израильской криптографии».

В начале 1990-х гг. вместе со своим учеником Э. Бихамом разрабатывает основу современных методов исследования и вскрытия блочных шифров – дифференциальный криптоанализ.

В 2007 г. А. Шамир заявил, что для современных криптосистем серьезная угроза таится в виде роста числа невыявленных ошибок, вызванных постоянным усложнением микропроцессоров. «Если спецслужбы обнаружат или скрытно внедрят в популярный микропроцессор алгоритм неправильного вычисления произведения только лишь одной пары чисел A и B (хотя бы в бите номер 0, т. е. наименее значимом бите), то любой ключ в любой RSA-программе на любом из миллионов ПК с этим чипом может быть взломан с помощью единственного сообщения», – пишет А. Шамир. Взлом может быть применен к любой системе, в которой задействованы открытые ключи, причем сейчас это не только ПК, но и телефоны и другие устройства.

W W W W W W W W W W W W W W W W W W W W W W W W W W W W W W W W

W W W В И К И С П Р А В К А W W W W W W W W W W W W W W W W W W W



Леонард Макс Адлеман
(англ. *Leonard Adleman*)
(род. 1945)

американский ученый-теоретик в области компьютерных наук, профессор компьютерных наук и молекулярной биологии.

Известен как соавтор системы шифрования RSA и ДНК-вычислений. В одном из интервью Л. Адлеман говорил: «Самое главное в ДНК-вычислениях – то, что они показывают, что молекулы ДНК могут сделать то, что, как мы обычно считаем, могут выполнить только компьютеры. Это означает, что компьютерная наука и биология тесно связаны. Каждое живое существо можно рассматривать как вычислительную систему, и порой мы можем понять живые существа лучше, рассматривая их в качестве компьютеров».

В 1983 г. предложил детерминированный алгоритм, использующий «почти полиномиальное время» для нахождения и различения простых чисел.
В 1993 г. описал математическую модель иммунной недостаточности, вызванной вирусом СПИДа.
Придумал термин «компьютерный вирус»; считал, что потенциально польза, полученная от компьютерных вирусов в технологиях будущего, может перевесить негативные стороны их использования.
W W W W W W W W W W W W W W W W W W W W W W W W W W W W W W

Алгоритм создания открытого и секретного ключей в криптосистеме RSA состоит из следуюших шагов.

1. Выбираются два различных случайных простых числа p и q.
2. Вычисляется модуль $m = pq$.
3. Вычисляется $\varphi(m) = (p-1)(q-1)$.
4. Выбирается целое число $e, 1 < e < \varphi(m)$, взаимно простое с $\varphi(m)$.
5. Вычисляется число d, удовлетворяющее $de \equiv 1 (\mathrm{mod}\, \varphi(m))$.

Открытый ключ RSA – пара (e, m); *закрытый ключ* – (d, m).

При шифровании допустимыми сообщениями являются числа N, $N < m, (N, m) = 1$. Зашифрованное сообщение вычисляется по формуле: $C \equiv N^e (\mathrm{mod} m)$.

При расшифровывании сообщение N вычисляется по зашифрованному сообщению C по формуле: $N \equiv C^d (\mathrm{mod}\, m)$.

Для взлома криптосистемы RSA необходимо определить закрытый ключ по открытому ключу, т. е. решить задачу факторизации целого числа m, представляющего собой произведение двух больших простых чисел p и q.

В 2002 г. Р. Ривесту, А. Шамиру и Л. Адлеману была присуждена премия Тьюринга с формулировкой «за уникальный вклад по увеличению практической пользы систем шифрования с открытым ключом».

В 1996 г. Л. Адлеман, У. Диффи, Р. Меркл, Р. Ривест, М. Хеллман и А. Шамир «за концепцию и первую эффективную реализацию криптосистем с открытым ключом» стали первыми лауреатами премии Париса Канеллакиса – ежегодной научной премии Ассоциации вычислительной техники, вручаемой за особые теоретические достижения, которые оказали значительное влияние на практическое развитие информационных технологий.

Понятие о первообразном корне по модулю m

Выше было отмечено, что в практической реализации классического алгоритма Диффи – Хеллмана при вычислении $A \equiv g^a (\mathrm{mod}\, p)$; $B \equiv g^b (\mathrm{mod}\, p)$ числа a и b выбирают большими, p – очень большим, но число g обычно невелико, при этом хорошо, если g является *первообразным корнем* по модулю p.

Опр. 1. Пусть $m \in \mathbb{N}, m > 1.$ Число $g \in \mathbb{Z},$ взаимно простое с m, называется ***первообразным корнем по модулю*** m, если $g^k \not\equiv 1 (\mathrm{mod}\, m)$ при всех k, $1 \le k < \varphi(m).$

Иными словами, $\varphi(m)$ – наименьшая положительная степень k, при которой $g^k \equiv 1 (\mathrm{mod}\, m).$

Согласно теореме Эйлера, $g^{\varphi(m)} \equiv 1 (\mathrm{mod}\, m)$ для любого g, $(g, m) = 1$. Однако значение функции Эйлера $\varphi(m)$ не всегда является наименьшим положительным значением k, при котором $g^k \equiv 1 (\mathrm{mod}\, m).$

Пример 1. Проверим, какие из чисел 2, 3, 4, 5 являются первообразными корнями по модулю $m = 13$.

Так как 13 – простое число, то $\varphi(13) = 12.$

Рассмотрим $g = 2.$ Вычислим:

$$2^1 \equiv 2 (\mathrm{mod} 13); \quad 2^2 \equiv 4 (\mathrm{mod} 13); \quad 2^3 \equiv 8 (\mathrm{mod} 13);$$

$$2^4 = 16 \equiv 3 (\mathrm{mod} 13); \quad 2^5 \equiv 3 \cdot 2 = 6 (\mathrm{mod} 13); \quad 2^6 \equiv 6 \cdot 2 = 12 (\mathrm{mod} 13);$$

$$2^7 \equiv 12 \cdot 2 \equiv 11 (\mathrm{mod} 13); \quad 2^8 \equiv 11 \cdot 2 \equiv 9 (\mathrm{mod} 13); \quad 2^9 \equiv 9 \cdot 2 \equiv 5 (\mathrm{mod} 13);$$

$$2^{10} \equiv 5 \cdot 2 = 10 (\mathrm{mod} 13); \quad 2^{11} \equiv 10 \cdot 2 \equiv 7 (\mathrm{mod} 13); \quad 2^{12} \equiv 7 \cdot 2 \equiv 1 (\mathrm{mod} 13).$$

Следовательно, $g = 2$ является первообразным корнем по модулю $m = 13$.

Поскольку

$$3^3 = 27 \equiv 1 (\mathrm{mod} 13); \quad 4^6 \equiv 1 (\mathrm{mod} 13); \quad 5^4 \equiv 1 (\mathrm{mod} 13),$$

то числа 3, 4, 5 не являются первообразными корнями по модулю $m = 13$. ●

Замечание. Первообразный корень по модулю m может быть не единственен. Можно показать, что числа 6, 7, 11 также являются первообразными корнями по модулю $m = 13$.

Как видно из примера 1, использование в криптосистеме Диффи – Хеллмана числа g, не являющегося первообразным корнем, приводит к суще-

ственному обеднению множества различных значений $A \equiv g^a (\mathrm{mod}\, p)$ и $B \equiv g^b (\mathrm{mod}\, p),$ что облегчает задачу дискретного логарифмирования и снижает криптографическую стойкость алгоритма.

Т 1. Если число g, $(g, m) = 1$, является первообразным корнем по модулю m, то числа $1, g, g^2, ..., g^{\varphi(m)-1}$ образуют приведенную систему вычетов по модулю m.

Интересно, однако, что первообразный корень по модулю m может не существовать.

Т 2 [Гаусс, 1801]. Первообразные корни по модулю m существуют тогда и только тогда, когда m – одно из чисел 2, 4, p^k, $2p^k$, где p – нечетное простое число, $k \in \mathbb{N}$.

Использование алгебраических структур для обобщения классических алгоритмов асимметричной криптографии

Революционный переворот, произведенный в криптографии в середине 1970-х гг. изобретением концепции несимметричных криптографических систем и введением в практику первых алгоритмов указанного типа, привел к стремительной алгебраизации криптографии и последующему вовлечению в теорию и практику все новых и новых алгебраических объектов: циклических групп, конечных полей, групп точек эллиптических кривых.

Классические алгоритмы асимметричной криптографии основаны на сравнениях по модулю. За счет развития вычислительной техники и методов криптоанализа для надежной защиты классических криптосистем требуется постоянно увеличивать длину ключа, что порождает множество проблем, особенно для узлов связи, специализирующихся на электронной коммерции, где требуется защита больших транзакций.

Поэтому в настоящее время используются модификации классических алгоритмов, основанные на действиях в конечных полях и в группах точек эллиптических кривых.

При построении криптоалгоритмов в конечных полях или на эллиптических кривых возведение в степень по большому модулю, определяющее стойкость шифра, фактически заменяется на возведение в степень порождающего элемента циклической группы. За счет использования более сложных алгебраических объектов обеспечиваются те же криптографические свойства при существенно меньшей длине ключа, а следовательно, упрощается программная и аппаратная реализация криптосистем.

§ 7. Группы

Понятие бинарной операции

Опр. 1. Пусть G – непустое множество. ***Бинарной алгебраической операцией*** на множестве G называется всякое правило, по которому каждой упорядоченной паре $(a;b)$ элементов $a,b\in G$ ставится в соответствие один вполне определенный элемент $c\in G$.

Замечание. Чтобы подчеркнуть тот факт, что для всех элементов $a,b\in G$ результат бинарной операции принадлежит множеству G, говорят, что множество G ***замкнуто относительно данной бинарной операции***.

Обычно операции обозначаются знаками $*$, $\times$, $\bullet$, $\circ$, $+$, $-$ и т. п. Воспользуемся первым из обозначений операции, тогда $c=a*b$.

На данном множестве G может быть задано, вообще говоря, много различных операций. Желая выделить одну или несколько из них, используют скобки $(G,*)$ и говорят, что операция $*$ определяет на G ***алгебраическую структуру*** или что $(G,*)$ – ***алгебраическая система***.

Пример 1. Так, на множестве целых чисел $\mathbb{Z}$ сложение, вычитание, умножение являются бинарными операциями и определяют различные алгебраические структуры $(\mathbb{Z},+)$, $(\mathbb{Z},-)$, $(\mathbb{Z},\times)$.

Можно также рассмотреть другие алгебраические структуры $(\mathbb{Z},\circ)$, $(\mathbb{Z},\bullet)$, введя новые бинарные операции на множестве $\mathbb{Z}$ равенствами

$$a\circ b=a+b-ab;\qquad a\bullet b=-a-b.\bullet$$

Алгебраические системы различают по операциям и свойствам этих операций.

Опр. 2. Бинарная операция $*$ на множестве G называется ***коммутативной***, если $a*b=b*a$ для всех $a,b\in G$.

Опр. 3. Бинарная операция $*$ на множестве G называется ***ассоциативной***, если $(a*b)*c=a*(b*c)$ для всех $a,b,c\in G$.

Пример 2. Операции сложения и умножения на множестве целых чисел $\mathbb{Z}$ являются коммутативными и ассоциативными.

Операция вычитания на $\mathbb{Z}$ не является ни коммутативной, ни ассоциативной. $\bullet$

Упражнение 1. Показать, что введенная в примере 1 на $\mathbb{Z}$ операция $\circ$ коммутативна и ассоциативна, а операция $\bullet$ коммутативна, но не ассоциативна.

Пример 3. Рассмотрим множество $M_n(\mathbb{R})$ всех квадратных матриц порядка $n>1$ с операциями сложения и умножения матриц.

Операция сложения матриц коммутативна и ассоциативна.

Операция умножения матриц является ассоциативной, но не является коммутативной.•

Опр. 4. Элемент $e \in G$ называется ***единичным*** (или ***нейтральным***) относительно бинарной операции *, если $e * a = a * e = a$ для всех $a \in G$.

Пример 4. Число 0 – нейтральный элемент относительно сложения на множестве целых чисел $\mathbb{Z}$.

Число 1 – нейтральный элемент относительно умножения в $\mathbb{Z}$.

Операция вычитания на множестве $\mathbb{Z}$ не имеет нейтрального элемента.•

Понятие группы

Опр. 5. ***Группой*** называется непустое множество G с определенной на нем бинарной алгебраической операцией *, которая обладает свойствами:

1) *ассоциативность* $(a * b) * c = a * (b * c)$ для любых $a, b, c \in G$;

2) существует *нейтральный* (*единичный*) элемент, т. е. такой элемент $e \in G$, что $e * a = a * e = a$ для каждого $a \in G$;

3) каждый элемент $a \in G$ имеет *обратный*, т. е. такой элемент $b \in G$, что $a * b = b * a = e$.

Опр. 6. Группа с коммутативной операцией называется ***коммутативной*** или ***абелевой группой***.

По количеству элементов группы делятся на *конечные* и *бесконечные*.

Опр. 7. Число элементов конечной группы G называется ***порядком группы*** и обозначается $|G|$.

Пример 5. **1)** $(\mathbb{Z},+),(\mathbb{Q},+),(\mathbb{R},+),(\mathbb{C},+)$ – множества целых, рациональных, вещественных, комплексных чисел с операцией сложения – бесконечные абелевы группы;

2) $(M_{m\times n}(\mathbb{R}),+)$ – множество прямоугольных $m\times n$ матриц ($m,n\in\mathbb{N}$ – фиксированные числа) с вещественными элементами относительно операции сложения матриц – бесконечная абелева группа;

3) $\mathrm{GL}_n(\mathbb{R})$ (General Linear Group – ***полная (общая) линейная группа***) – множество квадратных матриц порядка $n\geq 2$ с вещественными элементами и ненулевым определителем с операцией матричного умножения – бесконечная неабелева группа, так как произведение матриц не коммутативно;

4) $(\mathbb{Z}_m,+)$ – множество классов вычетов по натуральному модулю с операцией сложения – конечная абелева группа, $\left|\mathbb{Z}_m\right|=m.\bullet$

Замечание. Группы относительно операции сложения обычно называют ***аддитивными группами,*** при этом нейтральный элемент называют ***нулем*** и обозначают символом 0, а обратный к a элемент – ***противоположным*** и обозначают $-a$. Группы относительно операции умножения обычно называют ***мультипликативными группами,*** нейтральный элемент мультипликативной группы часто называют ***единицей***, а обратный к a элемент обозначают a^{-1}.

Пример 6. **1)** Примерами бесконечных мультипликативных абелевых групп являются $(\mathbb{Q}^*,\times),(\mathbb{R}^*,\times),(\mathbb{C}^*,\times)$ – множества рациональных, вещественных, комплексных чисел без нуля: $\mathbb{Q}^*=\mathbb{Q}\setminus\{0\},\ \mathbb{R}^*=\mathbb{R}\setminus\{0\},\mathbb{C}^*=\mathbb{C}\setminus\{0\}$.

2) Множество $\mathbb{Z}_m^*$ классов вычетов, взаимно простых с модулем m, с операцией умножения является конечной мультипликативной абелевой группой, $\left|\mathbb{Z}_m^*\right|=\varphi(m)$.

3) $\mathrm{GL}_n(\mathbb{R})$ (General Linear Group – *полная (общая) линейная группа*) – множество квадратных матриц порядка $n\geq 2$ с вещественными элементами и ненулевым определителем с операцией матричного умножения – бесконечная мультипликативная неабелева группа, так как произведение матриц не коммутативно.$\bullet$

Замечание. В конечных группах удобно задавать алгебраическую операцию с помощью таблицы Кэли.

Подгруппы

Опр. 8. Непустое подмножество H группы G называется ***подгруппой*** этой группы, если H само является группой относительно той же бинарной алгебраической операции.

Пример 7. 1) $(\mathbb{Z},+)\subset(\mathbb{Q},+)\subset(\mathbb{R},+)\subset(\mathbb{C},+)$;

2) $(\mathbb{Q}^*,\times)\subset(\mathbb{R}^*,\times)\subset(\mathbb{C}^*,\times)$;

3) $(\mathbb{Z},+)\supset(2\mathbb{Z},+)\supset(4\mathbb{Z},+)\supset(8\mathbb{Z},+)\supset\ldots\supset(2^k\mathbb{Z},+)\supset\ldots$, где $n\mathbb{Z}=\{nq: q\in\mathbb{Z}\}$, $k\in\mathbb{N}$.•

Т 1 (теорема Лагранжа). Порядок конечной группы делится на порядок любой ее подгруппы.

Циклические группы

Т 2. Пусть a – фиксированный элемент группы G. Тогда множество всевозможных целых степеней элемента a

$$< a >=\{a^0=e; a; a^2;\ldots; a^{-1}; a^{-2};\ldots\}=\{a^k, k\in\mathbb{Z}\}$$

является подгруппой группы G, причем эта подгруппа абелева.

Замечание. Под k-й степенью элемента группы понимается k-кратное применение бинарной операции группы к этому элементу, если $k>0$, и к его обратному элементу, если $k<0$:

$$a^k=\underbrace{a*a*\ldots*a}_{k\text{ множителей}};\quad a^{-k}=\underbrace{a^{-1}*a^{-1}*\ldots*a^{-1}}_{k\text{ множителей}},\ k\in\mathbb{N};\quad a^0=e.$$

При этом в силу ассоциативности бинарной операции группы

$$a^k*a^n=a^{k+n},\quad (a^k)^n=a^{kn},\ k,n\in\mathbb{Z}.$$

Опр. 9. Подгруппа $< a >$ называется ***циклической подгруппой, порожденной элементом*** a.

Пример 8. Рассмотрим группу $(\mathbb{Z}_7^*,\times)$ классов вычетов, взаимно простых с модулем 7, с операцией умножения и найдем подгруппы $<\overline{2}>,<\overline{3}>,<\overline{4}>$.

Группа $(\mathbb{Z}_7^*, \times) = \{\bar{1}; \bar{2}; \bar{3}; \bar{4}; \bar{5}; \bar{6}\}$.

Чтобы найти подгруппу $<\bar{2}>$, вычислим степени класса вычетов $\bar{2}$ по модулю 7:

$$\bar{2}^1 = \bar{2}; \quad \bar{2}^2 = \bar{4}; \quad \bar{2}^3 = \bar{1}.$$

Несложно понять, что далее все значения будут повторяться.

Поскольку $\bar{2}^1 \cdot \bar{2}^2 = \bar{2}^3 = \bar{1}$, заключаем, что $\bar{2}^{-1} = \bar{2}^2 = \bar{4}$ (обратным к элементу $\bar{2}$ в группе $(\mathbb{Z}_7^*, \times)$ является элемент $\bar{4}$). Так как

$$\bar{4}^1 = \bar{4}; \quad \bar{4}^2 = \bar{2}; \quad \bar{4}^3 = \bar{1},$$

поэтому $<\bar{2}>= \{\bar{2}, \bar{4}, \bar{1}\}$.

При этом $<\bar{4}>=<\bar{2}>= \{\bar{2}, \bar{4}, \bar{1}\}$.

Найдем подгруппу $<\bar{3}>$. Поскольку

$$\bar{3}^1 = \bar{3}; \quad \bar{3}^2 = \bar{2}; \quad \bar{3}^3 = \bar{6}; \quad \bar{3}^4 = \bar{4}; \quad \bar{3}^5 = \bar{5}; \quad \bar{3}^6 = \bar{1},$$

все элементы группы входят в $<\bar{3}>$, т. е. $<\bar{3}>= \mathbb{Z}_7^*$.●

Опр. 10. Группа G называется ***циклической***, если найдется такой элемент $b \in G$, что $G = <b>$, элемент b в этом случае называется ***образующим***.

Пример 8 (продолжение). Группа $(\mathbb{Z}_7^*, \times) = <\bar{3}>$ – циклическая, ее образующим является элемент $\bar{3}$.

Упражнение 2. Показать, что в качестве образующего этой группы может быть взят также элемент $\bar{5}$.●

Пример 9. 1) Группа $(\mathbb{Z}, +)$ является бесконечной циклической группой с образующим 1 или -1;

2) $(\mathbb{Z}_m, +)$ – конечная циклическая группа, порожденная элементом $\bar{1}$ или $\overline{-1}$.●

Замечание. $(\mathbb{Z}_m^*, \times)$ является циклической тогда и только тогда, когда по модулю m существует первообразный корень.

Пример 10. Покажем, что группа $(\mathbb{Z}_{18}^*, \times)$ является циклической.

Решение. Группа $(\mathbb{Z}_{18}^*,\times)$ – это группа классов вычетов по модулю 18, взаимно простых с модулем: $\mathbb{Z}_{18}^* = \left\{\bar{1};\bar{5};\bar{7};\overline{11};\overline{13};\overline{17}\right\}$.

Очевидно, что $<\bar{1}> = \{\bar{1}\} \neq \mathbb{Z}_{18}^*$.

Рассмотрим элемент $\bar{5}$. Поскольку

$$5^2 = 25 \equiv 7(\mathrm{mod}18);$$
$$5^3 \equiv 7\cdot 5 = 35 \equiv 17(\mathrm{mod}18);$$
$$5^4 \equiv 17\cdot 5 \equiv (-1)\cdot 5 = -5 \equiv 13(\mathrm{mod}18);$$
$$5^5 \equiv 13\cdot 5 \equiv (-5)\cdot 5 = -25 \equiv 11(\mathrm{mod}18);$$
$$5^6 \equiv 11\cdot 5 = 55 \equiv 1(\mathrm{mod}18),$$

$<\bar{5}> = \left\{\bar{5};\bar{7};\overline{17};\overline{13};\overline{11};\bar{1}\right\} = \mathbb{Z}_{18}^*$ и группа $(\mathbb{Z}_{18}^*,\times)$ является циклической. •

Т 3. Всякая циклическая группа абелева.

Доказательство. Для произвольных элементов группы $<a>$ в силу ассоциативности операции в группе имеем $a^k * a^n = a^{k+n} = a^{n+k} = a^n * a^k$. ◁

Т 4. Всякая подгруппа циклической группы является циклической.

Доказательство. Пусть $G = <a>$ и H – подгруппа этой группы, отличная от G и $\{e\}$. Тогда найдется натуральное k такое, что $a^k \in H$. Возьмем такое наименьшее натуральное k, что $a^k \in H$, и покажем, что $H = <a^k>$.

Для произвольного элемента $h \in H$, поскольку он также является элементом циклической группы $G = <a>$, найдется такое целое s, что $h = a^s$. По теореме о делении с остатком $s = kq + r$, где q, r – целые числа, $0 \le r < k$. Тогда $h = (a^k)^q * a^r$. Следовательно, $a^r = h * (a^k)^{-q} \in H$, что, в силу минимальности k возможно только при $r = 0$. Значит, всякий элемент $h \in H$ представим в виде $h = (a^k)^q$ и $H = <a^k>$. ◁

Порядок элемента группы

Опр. 11. Натуральное число n называется ***порядком элемента*** $a \in G$, если $a^n = e$ и $a^k \neq e$ для всех натуральных $k, 1 \le k < n$.

Если $a^k \neq e$ при всех натуральных k, то элемент $a \in G$ называется ***элементом бесконечного порядка***.

Пример 11. 1) Элемент 1 в группе $(\mathbb{Z},+)$ имеет бесконечной порядок;

2) элемент $\overline{1}$ в группе $(\mathbb{Z}_m,+)$ имеет порядок m.•

Т 5. Если $a \in G$ имеет порядок n, то циклическая подгруппа $< a >$ имеет порядок n и

$$\boxed{< a > = \{a; a^2; ...; a^n = e\}.}$$

Доказательство. Для любого целого k, разделив его с остатком на n, получим $k = nq + r$, где – целые числа, $0 \le r < n$, откуда

$$a^k = (a^n)^q * a^r = e^q * a^r = a^r,$$

т. е. любой элемент циклической подгруппы $< a >$ представим в виде a^r, где $0 \le r < n$. ◁

Пример 12. 1) Рассмотрим группу $< A >$, порожденную матрицей $A = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{R})$ (т. к. $\det A = 1 \neq 0$).

Вычислим

$$A^2 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1\cdot 1 + 2\cdot 0 & 1\cdot 2 + 2\cdot 1 \\ 0\cdot 1 + 1\cdot 0 & 0\cdot 2 + 1\cdot 1 \end{pmatrix} = \begin{pmatrix} 1 & 4 \\ 0 & 1 \end{pmatrix};$$

$$A^3 = A^2 A = \begin{pmatrix} 1 & 4 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1\cdot 1 + 4\cdot 0 & 1\cdot 2 + 4\cdot 1 \\ 0\cdot 1 + 1\cdot 0 & 0\cdot 2 + 1\cdot 1 \end{pmatrix} = \begin{pmatrix} 1 & 6 \\ 0 & 1 \end{pmatrix}$$

и т. д.

Найдем обратную матрицу, используя формулу

$$A^{-1} = \frac{1}{\det A}\begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix}^T,$$

где $\det A$ – определитель матрицы A, а $A_{ij} = (-1)^{i+j} M_{ij}$ – алгебраическое дополнение элемента a_{ij} матрицы A, которое равно, с точностью знака, определителю, полученному из определителя мат-

рицы A путем вычеркивания i-й строки и j-го столбца, т. е. строки и столбца, в которых стоит элемент a_{ij}. Итак, поскольку

$$\det A = 1\cdot 1 - 0\cdot 1 = 1;$$

$$A_{11} = 1; \quad A_{12} = 0;$$
$$A_{21} = -2; \quad A_{22} = 1,$$

то обратная матрица равна $A^{-1} = \begin{pmatrix} 1 & -2 \\ 0 & 1 \end{pmatrix}$.

Таким образом,

$$A^2 = \begin{pmatrix} 1 & 4 \\ 0 & 1 \end{pmatrix}, A^3 = \begin{pmatrix} 1 & 6 \\ 0 & 1 \end{pmatrix}, ..., A^{-1} = \begin{pmatrix} 1 & -2 \\ 0 & 1 \end{pmatrix}, A^{-2} = \begin{pmatrix} 1 & -4 \\ 0 & 1 \end{pmatrix}, ...,$$

т. е. степени матрицы A попарно различны и образуют бесконечную последовательность. Таким образом, циклическая подгруппа, порожденная матрицей A в группе $\mathrm{GL}_2(\mathbb{R})$, является бесконечной.

2) Матрица $H \in \mathrm{GL}_2(\mathbb{R})$ вида $H = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ имеет степени

$$H^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, H^3 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, H^4 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = E,$$

где E – единичная матрица. Согласно теореме 5, подгруппа $< H >$ – конечная подгруппа порядка 4.•

Замечание. Отметим, что чаще группы не являются циклическими. Например, все некоммутативные группы не могут быть циклическими.

Следствие теоремы Лагранжа. Порядок элемента группы делит порядок группы. Если G – конечная группа из n элементов, то $a^n = e$ для каждого $a \in G$.

Доказательство. Пусть $|G| = n$. Если $a = e$, то $e^n = e$. Если $a \neq e$, то рассмотрим $< a >$ и обозначим $|< a >| = k$. По теореме 1, $n = kq$, где q – целое. По теореме 5, порядок циклической подгруппы $< a >$ равен порядку элемента $a \in G$, поэтому порядок

элемента a равен k, т. е. $a^k = e,$ а следовательно, $a^n = (a^k)^q = e^q = e.$ $\triangleleft$

Пример 13. Покажем, что группа $(\mathbb{Z}_{36}^*,\times)$ не является циклической.

Решение. Группа $(\mathbb{Z}_{36}^*,\times)$ – это группа классов вычетов по модулю 36, взаимно простых с модулем:

$$G = \mathbb{Z}_{36}^* = \left\{ \bar{1}; \bar{5}; \bar{7}; \overline{11}; \overline{13}; \overline{17}; \overline{19}; \overline{23}; \overline{25}; \overline{29}; \overline{31}; \overline{35} \right\},$$

порядок этой группы равен $|G| = \varphi(36) = \varphi(2^2 \cdot 3^2) = 12.$

Чтобы показать, что эта группа не является циклической, нужно показать, что для каждого элемента $a \in \mathbb{Z}_{36}^*$ циклическая группа $< a > = \{a^0 = e; a; a^2; ...\},$ порожденная этим элементом, не совпадает с $G = \mathbb{Z}_{36}^*.$

Очевидно, что $< \bar{1} > = \{\bar{1}\} \neq \mathbb{Z}_{36}^*.$

Рассмотрим $a = \bar{5}.$ Поскольку

$$5^2 = 25 (\mathrm{mod}\, 36);$$
$$5^3 = 125 \equiv 17 (\mathrm{mod}\, 36);$$
$$5^4 \equiv 17 \cdot 5 = 85 \equiv 13 (\mathrm{mod}\, 36);$$
$$5^5 \equiv 13 \cdot 5 = 65 \equiv 29 (\mathrm{mod}\, 36);$$
$$5^6 \equiv 29 \cdot 5 = 145 \equiv 1 (\mathrm{mod}\, 36),$$

то $< \bar{5} > = \left\{ \bar{1}; \bar{5}; \overline{13}; \overline{17}; \overline{25}; \overline{29} \right\}$ – подгруппа порядка 6 в группе $\mathbb{Z}_{36}^*$ порядка 12. По следствию из теоремы Лагранжа все остальные элементы этой подгруппы имеют порядки, являющиеся делителями 6.

Рассмотрим элемент $a = \bar{7},$ не принадлежащий подгруппе $< \bar{5} >.$ Поскольку

$$7^2 = 49 \equiv 13 (\mathrm{mod}\, 36);$$
$$7^3 \equiv 13 \cdot 7 = 91 \equiv 19 (\mathrm{mod}\, 36);$$
$$7^4 \equiv 19 \cdot 7 = 133 \equiv 25 (\mathrm{mod}\, 36);$$

$$7^5 \equiv 25 \cdot 7 = 175 \equiv 31 (\mathrm{mod}\, 36);$$
$$7^6 \equiv 31 \cdot 7 = 217 \equiv 1 (\mathrm{mod}\, 36),$$

то $< \overline{7} > = \left\{ \overline{1}; \overline{7}; \overline{13}; \overline{19}; \overline{25}; \overline{31} \right\}$ – подгруппа порядка 6. Следовательно, ее элементы $\overline{7}, \overline{19}, \overline{31},$ не принадлежащие $< \overline{5} >,$ также имеют порядок, не превышающий 6.

Рассмотрим $a = \overline{11}$:

$$11^2 = 121 \equiv 13 (\mathrm{mod}\, 36);$$
$$11^3 \equiv 13 \cdot 11 = 143 \equiv 35 (\mathrm{mod}\, 36);$$
$$11^4 \equiv 35 \cdot 11 \equiv (-1) \cdot 11 = -11 \equiv 25 (\mathrm{mod}\, 36);$$
$$11^5 \equiv 25 \cdot 11 \equiv (-11) \cdot 11 = -121 \equiv 23 (\mathrm{mod}\, 36);$$
$$11^6 \equiv 23 \cdot 11 \equiv (-13) \cdot 11 = -143 \equiv 1 (\mathrm{mod}\, 36).$$

Таким образом, $< \overline{11} > = \left\{ \overline{1}; \overline{11}; \overline{13}; \overline{23}; \overline{25}; \overline{35} \right\}$ – подгруппа порядка 6. Следовательно, ее элементы $\overline{11}, \overline{23}, \overline{35},$ не принадлежащие подгруппам $< \overline{7} >$ и $< \overline{5} >,$ также имеют порядок, не превышающий 6.

Таким образом, все 12 элементов группы $\mathbb{Z}_{36}^*$ имеют порядок, не превосходящий 6. Поэтому группа $\mathbb{Z}_{36}^*$ не может быть циклической.•

Изоморфизмы групп

Пусть $(G_1, *)$ и $(G_2, \circ)$ – две группы (в каждой группе определена своя операция $*$ или $\circ$).

Опр. 12. Взаимно однозначное отображение $f : G_1 \to G_2,$ сохраняющее операцию, т. е. обладающее свойством $f(a * b) = f(a) \circ f(b)$ для всех $a, b \in G_1,$ называется ***изоморфизмом групп*** G_1 ***и*** G_2. Изоморфные группы обозначают $G_1 \cong G_2$.

В математике изоморфные объекты считаются одинаковыми. Основная цель теории групп – классифицировать все группы с точностью до изоморфизма.

Утв. 1. Если $f: G_1 \to G_2$ – изоморфизм групп, то:

1) $f(e_1) = e_2$, т. е. при изоморфизме нейтральный элемент первой группы переходит в нейтральный элемент второй группы;

2) $f(a^{-1}) = (f(a))^{-1}$ для всех $a \in G_1$, т. е. образ обратного элемента при изоморфизме есть обратный элемент к образу.

Т 6. Все циклические группы одного и того же порядка изоморфны.

§ 8. Кольца. Поля

Опр. 1. ***Кольцо*** – непустое множество K с двумя бинарными алгебраическими операциями + (сложение) и · (умножение), такими, что:

1) K является *абелевой группой* относительно операции сложения +;

2) операция *умножения ассоциативна*, т. е.

$$(a \cdot b) \cdot c = a \cdot (b \cdot c) \text{ для всех } a, b, c \in K;$$

3) операции умножения и сложения связаны законами *дистрибутивности* (умножение дистрибутивно по сложению): для произвольных $a, b, c \in K$

$$(a + b) \cdot c = a \cdot c + b \cdot c;$$
$$c \cdot (a + b) = c \cdot a + c \cdot b.$$

Условимся нейтральный элемент аддитивной группы кольца называть ***нулем*** и обозначать символом 0; противоположный к элементу a элемент обычно обозначают через $-a$; вместо $a + (-b)$ пишут $a - b$. Знак · операции умножения при записи произведений элементов кольца будем, как правило, опускать.

Пример 1. 1) $(\mathbb{Z}, +, \cdot)$ – кольцо целых чисел.

2) $(\mathbb{Z}_m, +, \cdot)$ – кольцо классов вычетов по модулю $m > 1$.

3) Множество всех вещественных функций, определенных на данном интервале $(a; b)$ числовой оси с обычными операциями сложения и умножения функций.

4) Кольцо $\mathbb{R}[x]$ полиномов (многочленов) с вещественными коэффициентами от переменной x с естественными операциями сложения и умножения.

5) Множество всех квадратных матриц данного порядка n с элементами из $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ или $\mathbb{C}$ с операциями матричного сложения и умножения.●

Опр. 2. Кольцо K называется ***коммутативным***, если операция умножения в нем коммутативна, т. е. $ab = ba$ для всех $a, b \in K$.

Опр. 3. Кольцо K называется ***кольцом с единицей***, если оно имеет мультипликативную единицу, т. е. такой элемент e, что $ea = ae = a$ для каждого $a \in K$.

Пример 2. Все кольца из примеров **1.1)**–**4)** являются коммутативными кольцами с единицей.

Множество квадратных матриц данного порядка (пример **1.5)**) представляет собой пример некоммутативного кольца с единицей.

Примером коммутативного кольца без единицы является при $m > 1$ кольцо $m\mathbb{Z} = \{ma : a \in \mathbb{Z}\}$ – множество целых чисел, кратных m. ●

Утв. 1. Если K – кольцо с единицей, содержащее более одного элемента, то в нем $e \neq 0$ (единичный элемент не равен нулю).

Доказательство. Так как K содержит более одного элемента и нулевой элемент $0 \in K$, то найдется еще один элемент кольца $a \neq 0$.

Если допустить, что $e = 0$, то из $ae = a \cdot 0 = 0$ следует, что a = 0, т. е. приходим к противоречию. Значит, предположение неверно и $e \neq 0$. ◁

Опр. 4. Если в кольце K найдутся *ненулевые* элементы a и b такие, что $ab = 0$, то их называют ***делителями нуля***.

Пример 3. 1) Кольца чисел $(\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C})$ – кольца без делителей нуля.

2) В кольце классов вычетов $\mathbb{Z}_m$ с $m = pq$ классы $\overline{p}$ и $\overline{q}$ являются делителями нуля.

3) В кольце матриц $M_3(\mathbb{R})$ примерами делителей нуля являются матрицы $A = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$ и $B = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$, так как $AB = O$. •

Утв. 2. В кольце с единицей делители нуля не обратимы.

Доказательство. Пусть ненулевые элементы $a, b \in K$ являются делителями нуля, т. е. произведение $ab = 0$ и $a \neq 0$, $b \neq 0$. Если предположить что один из делителей нуля b обратим, т. е. существует $b^{-1} \in K$, то, с одной сто-

роны, $(ab)b^{-1}=0,$ а с другой, $(ab)b^{-1}=a(bb^{-1})=ae=a,$ т. е. a = 0, что противоречит сделанному предположению. ◁

Т 1. Если K – кольцо с единицей, то множество K^* обратимых относительно умножения элементов кольца K есть группа относительно умножения.

Доказательство. 1) Проверим аксиомы группы.

1. Умножение в K^* ассоциативно, так как K – кольцо, и умножение в нем ассоциативно, а K^* – подмножество множества K.

2. Если e – нейтральный элемент кольца K относительно умножения, то $e\cdot e=e,$ т. е. обратным к e элементом является $e \Rightarrow e\in K^*$.

3. Для любого $a\in K^*$ обратный элемент $a^{-1}\in K^*,$ так как $a^{-1}a=aa^{-1}=e\in K^*,$ а значит, $(a^{-1})^{-1}=a,$ элемент a^{-1} обратим, поэтому $a^{-1}\in K^*$.

2) Проверим, что множество K^* замкнуто относительно умножения.

Пусть $a,b\in K^*$ и $a^{-1},$ b^{-1} – обратные элементы к a и b соответственно, причем $a^{-1},b^{-1}\in K^*$. Покажем, что $ab\in K^*,$ т. е. что элемент ab имеет обратный. Поскольку

$$(ab)(b^{-1}a^{-1})=a(bb^{-1})a^{-1}=aea^{-1}=e;$$
$$(b^{-1}a^{-1})(ab)=b^{-1}(a^{-1}a)b=b^{-1}eb^{-1}=e,$$

то обратным к элементу $ab\in K$ является элемент $b^{-1}a^{-1}\in K,$ а значит, $ab\in K^*$. ◁

Опр. 5. Множество K^* обратимых относительно умножения элементов кольца K называют ***мультипликативной группой кольца*** *K.*

Пример 4. 1) В кольце целых чисел $\mathbb{Z}$ обратимы относительно умножения только два числа: 1 и $-1,$ поэтому $\mathbb{Z}^*=\{\pm1\}$.

2) $\mathbb{Q}^*=\mathbb{Q}\setminus\{0\},\mathbb{R}^*=\mathbb{R}\setminus\{0\},\mathbb{C}^*=\mathbb{C}\setminus\{0\}.$

3) В кольце $M_n(\mathbb{R})$ квадратных матриц порядка n обратимы только матрицы с ненулевым определителем, поэтому $M_n(\mathbb{R})^*=\mathrm{GL}_n(\mathbb{R}).$

4) В кольце $\mathbb{Z}_m$ множество $\mathbb{Z}_m^*$ обратимых классов вычетов содержит классы вычетов, взаимно простых с модулем, т. е. $\mathbb{Z}_m^* = \{\overline{k} : (k,m) = 1\}$, причем $|\mathbb{Z}_m^*| = \varphi(m)$. •

Опр. 6. ***Поле*** – коммутативное кольцо с единицей, в котором каждый ненулевой элемент обратим.

Пример 5. 1) $\mathbb{Q}$ – поле рациональных чисел, $\mathbb{R}$ – поле вещественных чисел, $\mathbb{C}$ – поле комплексных чисел с естественными операциями сложения и умножения.

2) Множество классов вычетов $\mathbb{Z}_m$ является полем тогда и только тогда, когда $m = p$ – простое число. При этом $\mathbb{Z}_p$ – конечное поле из p элементов. •

Свойства полей.

1. В поле нет делителей нуля.

Доказательство. Допустим, в поле P существуют делители нуля $a, b \in P$, т. е. произведение $ab = 0$ и $a \neq 0$, $b \neq 0$. Поскольку в поле каждый ненулевой элемент обратим, то существует $a^{-1} \in P^*$. Тогда, с одной стороны, $a^{-1}(ab) = a^{-1} \cdot 0 = 0$, а с другой, $a^{-1}(ab) = (a^{-1}a)b = eb = b$, откуда получаем, что $b = 0$, что противоречит предположению. Следовательно, в поле нет делителей нуля. ◁

2. Мультипликативная группа поля содержит все его ненулевые элементы: $P^* = P \setminus \{0\}$.

3. Если $(P,+,\cdot)$ – поле, то $(P,+)$ – аддитивная абелева группа, $(P^*,\cdot)$ – мультипликативная абелева группа. (Здесь $P^* = P \setminus \{0\}$.)

Подкольца. Подполя

Опр. 7. Подмножество R кольца K называется ***подкольцом*** этого кольца, если оно замкнуто относительно имеющихся в K операций сложения и умножения и само является кольцом относительно этих операций.

Пример 6. 1) $R = \{0\}$, $R = K$ – ***тривиальные*** (***несобственные***) подкольца любого кольца K.

2) Кольцо целых чисел $\mathbb{Z}$ – подкольцо кольца $\mathbb{Q}$ рациональных чисел; $\mathbb{Q}$ – подкольцо кольца $\mathbb{R}$ вещественных чисел, $\mathbb{R}$ –

подкольцо кольца $\mathbb{C}$ комплексных чисел. (Все эти кольца коммутативны.)

3) $M_n(\mathbb{Z}) \subset M_n(\mathbb{Q}) \subset M_n(\mathbb{R}) \subset M_n(\mathbb{C})$. (При $n > 1$ все эти кольца некоммутативны.)

4) Кольцо $m\mathbb{Z}$ целых чисел, кратных m, – подкольцо кольца $\mathbb{Z}$ целых чисел, причем $m\mathbb{Z}$ – это кольцо без единицы (при $m > 1$), хотя само кольцо $\mathbb{Z}$ с единицей.

5) Матричное кольцо $M_2(\mathbb{R})$ содержит подкольцо матриц $\left\{\begin{pmatrix} a & b \\ -b & a \end{pmatrix} : a, b \in \mathbb{R}\right\}$, которое в свою очередь содержит подкольцо скалярных матриц $\left\{\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} : a \in \mathbb{R}\right\}$. Отметим, что это коммутативные подкольца некоммутативного кольца $M_2(\mathbb{R})$.•

Опр. 8. Подмножество F поля P называется ***подполем*** поля P, если оно замкнуто относительно имеющихся операций сложения и умножения и само является полем относительно этих операций. При этом поле P называют ***расширением*** поля F.

Подполе F называется ***собственным подполем*** поля P, если $F \neq P$.

Пример 7. Поле рациональных чисел $\mathbb{Q}$ является собственным подполем поля вещественных чисел $\mathbb{R}$, которое в свою очередь будет собственным подполем поля комплексных чисел $\mathbb{C}$.•

Изоморфизмы колец и полей

Пусть K_1, K_2 – два кольца.

Опр. 9. Взаимно однозначное отображение $f : K_1 \to K_2$, сохраняющее операции, т. е. обладающее свойствами $f(a+b) = f(a) + f(b),\ f(ab) = f(a)f(b)$ для всех $a, b \in K_1$, называется ***изоморфизмом колец*** K_1 ***и*** K_2. Изоморфные кольца обозначают $K_1 \cong K_2$.

Утв. 3. Если $f : K_1 \to K_2$ – изоморфизм колец, то:

1) $f(0_1) = 0_2$, т. е. при изоморфизме нулевой элемент первого кольца переходит в нулевой элемент второго кольца;

2) $f(-a)=-f(a)$ для всех $a\in K_1$, т. е. образ противоположного элемента при изоморфизме есть противоположный элемент к образу;

3) $f(e_1)=e_2$, т. е. при изоморфизме единица первого кольца переходит в единицу второго кольца;

4) $f(a^{-1})=\big(f(a)\big)^{-1}$ для всех $a\in K_1$, т. е. образ обратного элемента при изоморфизме есть обратный элемент к образу.

Опр. 10. Поля P_1 и P_2 называются ***изоморфными*** ($P_1\cong P_2$), если они изоморфны как кольца.

Утв. 4. Пересечение любого количества подполей данного поля P также является подполем P.

Опр. 11. Поле, не содержащее собственных подполей, называется ***простым*** или ***минимальным***.

Т 2. В каждом поле P содержится одно и только одно простое подполе F. Это поле F изоморфно либо полю $\mathbb{Q}$, либо полю $\mathbb{Z}_p$ при некотором простом p.

Конечные поля, или поля Галуа

Опр. 12. Поле P называется ***конечным***, если число его элементов конечно. Число элементов в поле называется его ***порядком***.

Пример 8. 1) Поле $\mathbb{Q}$ рациональных чисел, поле $\mathbb{R}$ вещественных чисел, поле $\mathbb{C}$ комплексных чисел – бесконечные поля, причем $\mathbb{Q}\subset\mathbb{R}\subset\mathbb{C}$.

2) Поле классов вычетов $\mathbb{Z}_p$ – конечное поле из p элементов, если p – простое число.•

Конечное поле порядка q обозначается $\mathbb{F}_q$ или GF(q) (сокращение от *Galois Field*) и называется полем Галуа; понятие конечного поля в его общем значении (когда имеются в виду не только поля, изоморфные $\mathbb{Z}_p$) впервые появилось в 1830 г. в статье Э. Галуа.

Эвари́ст Галуа́
(фр. *Évariste Galois*)
(1811–1832)
французский математик. Радикальный революционер-республиканец, был застрелен на дуэли в возрасте двадцати лет. В ночь перед дуэлью Галуа написал длинное письмо, в котором кратко изложил итоги своих исследований.

Открытия Галуа положили начало теории абстрактных алгебраических структур. Теперь объединяющий подход Галуа признан одним из самых выдающихся достижений математики XIX в. Теория Галуа – раздел алгебры, позволяющий переформулировать определенные вопросы теории полей на языке теории групп, делая их в некотором смысле более простыми.

Построение конечного поля как множества классов вычетов по модулю неприводимого многочлена с коэффициентами из $\mathbb{Z}_p$

Рассмотрим множество многочленов с коэффициентами из $\mathbb{Z}_p$:

$$\mathbb{Z}_p[x] = \left\{ a(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n : n \in \mathbb{N}, a_0, a_1, a_2, \ldots, a_n \in \mathbb{Z}_p \right\}.$$

Операции сложения и умножения элементов $\mathbb{Z}_p[x]$ определяются обычным образом с учетом того, что все действия над коэффициентами осуществляются в $\mathbb{Z}_p$ (по модулю p).

Утв. 5. $\mathbb{Z}_p[x]$ (p – простое) является коммутативным кольцом с единицей и без делителей нуля, но не является полем.

Элементы поля $\mathbb{Z}_p$ также являются элементами кольца $\mathbb{Z}_p[x]$, поскольку могут рассматриваться как многочлены нулевой степени. Отметим, что нулевым и единичным элементами кольца $\mathbb{Z}_p[x]$ являются соответственно нулевой $\bar{0}$ и единичный $\bar{1}$ элементы поля $\mathbb{Z}_p$, а обратимыми элементами кольца $\mathbb{Z}_p[x]$ являются только ненулевые элементы поля $\mathbb{Z}_p$.

Т 3 (о делении с остатком). Для любых $a(x), b(x) \in \mathbb{Z}_p[x]$, где $b(x) \neq \bar{0}$, существуют и единственны $q(x), r(x) \in \mathbb{Z}_p[x]$, такие, что

$$a(x) = b(x)q(x) + r(x), \text{ где } 0 \le \deg r(x) < \deg b(x) \text{ или } r(x) = \bar{0}.$$

В этом случае многочлен $r(x)$ называется ***остатком от деления*** $a(x)$ ***на*** $b(x)$.

Пусть $m(x) \in \mathbb{Z}_p[x]$ – фиксированный многочлен степени $n \ge 1$. Рассматривая различные остатки от деления на $m(x)$ в $\mathbb{Z}_p[x]$, можно разбить множество $\mathbb{Z}_p[x]$ на классы эквивалентности – классы вычетов по модулю $m(x)$.

Опр. 13. ***Классом вычетов по модулю*** $m(x)$ называется множество всех многочленов из $\mathbb{Z}_p[x]$, имеющих один и тот же остаток от деления на $m(x)$, т. е.

$$\overline{r(x)} = \left\{ a(x) \in \mathbb{Z}_p[x] : a(x) = m(x)q(x) + r(x), \deg r(x) < \deg m(x) \text{ или } r(x) = \bar{0} \right\}.$$

Опр. 14. Множество всех классов сравнимых друг с другом по модулю $m(x)$ многочленов из $\mathbb{Z}_p[x]$ называют ***множеством классов вычетов по модулю*** $m(x)$ и обозначают через $\mathbb{Z}_p[x]/(m(x))$.

Отметим, что множество $\mathbb{Z}_p[x]/(m(x))$ содержит конечное число элементов. Действительно, если $\deg m(x) = n$, то остатками от деления на $m(x)$ могут быть только многочлены степени меньше n, причем каждый коэффициент – это элемент $\mathbb{Z}_p$, т. е. выби-

рается из p вариантов. Можно показать, что множество $\mathbb{Z}_p[x]/(m(x))$, где $\deg m(x) = n$, содержит p^n элементов.

Пример 9. $\mathbb{Z}_2[x]/(x^2+x) = \left\{\overline{0}; \overline{1}; \overline{x}; \overline{x+1}\right\}$. •

На множестве $\mathbb{Z}_p[x]/(m(x))$ классов вычетов по заданному модулю $m(x)$ можно ввести арифметические операции сложения и умножения, определяя их соответствующими операциями над представителями этих классов, а затем при необходимости вычисляя остаток от деления результата на модуль $m(x)$.

Пример 9 (продолжение). Вычислим $\overline{x} + \overline{x+1}; \overline{x+1} + \overline{x+1}; \overline{x} \cdot \overline{x+1}; \overline{x+1} \cdot \overline{x+1}$ в $\mathbb{Z}_2[x]/(x^2+x)$.

Решение. Помня, что все действия осуществляются над полем $\mathbb{Z}_2$, т. е. по модулю 2, вычисляем

$$\overline{x} + \overline{x+1} = \overline{x+x+1} = \overline{2x+1} = \overline{0x+1} = \overline{1};$$

$$\overline{x+1} + \overline{x+1} = \overline{x+1+x+1} = \overline{2x+2} = \overline{0x+0} = \overline{0}.$$

Умножая, получим

$$\overline{x} \cdot \overline{x+1} = \overline{x(x+1)} = \overline{x^2+x};$$

$$\overline{x+1} \cdot \overline{x+1} = \overline{(x+1)^2} = \overline{x^2+2x+1} = \overline{x^2+1}.$$

Переходя к остаткам от деления на x^2+x, окончательно имеем

$$\overline{x} \cdot \overline{x+1} = \overline{x^2+x} = \overline{0};$$

$$\overline{x+1} \cdot \overline{x+1} = \overline{x^2+1} = \overline{x+1},$$

так как $x^2+1 = (x^2+x)\cdot 1 + x + 1$ в $\mathbb{Z}_2[x]$. •

Опр. 15. Многочлен $m(x) \in \mathbb{Z}_p[x]$ степени $n \geq 1$ называется ***неприводимым*** в кольце $\mathbb{Z}_p[x]$ (или над полем $\mathbb{Z}_p$), если в любом его представлении $m(x) = b(x)q(x)$ в виде произведения двух многочленов $b(x), q(x) \in \mathbb{Z}_p[x]$ один из сомножителей является константой, т. е. элементом поля $\mathbb{Z}_p$.

Т 4. 1) Множество $\mathbb{Z}_p[x]/(m(x))$ классов вычетов по модулю многочлена $m(x)$ является коммутативным кольцом с единицей.

2) Если многочлен $m(x)$ неприводим над полем $\mathbb{Z}_p$ (p – простое), то множество $\mathbb{Z}_p[x]/(m(x))$ классов вычетов по модулю $m(x)$ является конечным полем, причем порядок этого поля равен p^n, где $n = \deg m(x)$.

Пример 9 (продолжение). Многочлен $x^2 + x$ не является неприводимым над $\mathbb{Z}_2$, так как $x^2 + x = x(x+1)$. Следовательно, кольцо $\mathbb{Z}_2[x]/(x^2 + x)$ не является полем.

Действительно, как было показано выше, в кольце $\mathbb{Z}_2[x]/(x^2 + x)$ имеются делители нуля, так как $\bar{x} \cdot \overline{x+1} = \bar{0}$. ●

Упражнение. Показать, что многочлен $x^2 + 1$ не является неприводимым над $\mathbb{Z}_2$.

Пример 10. Составим таблицы Кэли сложения и умножения в $F = \mathbb{Z}_2[x]/(x^2 + x + 1)$.

Решение. Кольцо состоит из классов эквивалентности $\bar{0}, \bar{1}, \bar{x}, \overline{x+1}$, поскольку это все возможные многочлены нулевой и первой степени в кольце $\mathbb{Z}_2[x]$.

$\oplus$	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\overline{x+1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\overline{x+1}$
$\bar{1}$	$\bar{1}$	$\bar{0}$	$\overline{x+1}$	$\bar{x}$
$\bar{x}$	$\bar{x}$	$\overline{x+1}$	$\bar{0}$	$\bar{1}$
$\overline{x+1}$	$\overline{x+1}$	$\bar{x}$	$\bar{1}$	$\bar{0}$

$\otimes$	$\bar{1}$	$\bar{x}$	$\overline{x+1}$
$\bar{1}$	$\bar{1}$	$\bar{x}$	$\overline{x+1}$
$\bar{x}$	$\bar{x}$	$\overline{x+1}$	$\bar{1}$
$\overline{x+1}$	$\overline{x+1}$	$\bar{1}$	$\bar{x}$

Из таблицы умножения видно, что в кольце F все элементы из $F \setminus \{\bar{0}\}$ обратимы относительно умножения, т. е. $F^* = F \setminus \{\bar{0}\}$. Следовательно, F – поле из четырех элементов.●

Характеристика поля

Опр. 16. Если для поля P существует такое натуральное n, что сумма n единиц поля (n раз складывается с самим собой нейтральный относительно умножения элемент поля) равна 0 (нейтральному элементу относительно сложения), то наименьшее n с таким свойством называется ***характеристикой поля*** P и обозначается $\operatorname{char} P$. Если в поле P любая конечная сумма единиц отлична от нуля, то говорят, что характеристика поля равна 0.

Пример 11. 1) $\operatorname{char}\mathbb{Q} = \operatorname{char}\mathbb{R} = \operatorname{char}\mathbb{C}$.

2) $\operatorname{char}\mathbb{Z}_p = p$.

3) Если $m(x)$ – неприводимый многочлен степени n над полем $\mathbb{Z}_p$, то $F = \mathbb{Z}_p[x]/(m(x))$ – конечное поле порядка p^n, однако $\operatorname{char} F = p$, поскольку единица и ноль этого поля представляют собой классы многочленов, имеющих при делении на $m(x)$ остатки, равные соответственно единице и нулю поля $\mathbb{Z}_p$, поэтому сумма p единиц равна 0. •

Пример 12. Примером бесконечного по количеству элементов поля конечной характеристики является поле рациональных функций над $\mathbb{Z}_p$:

$$\mathbb{Z}_p(x) = \left\{ \frac{a(x)}{b(x)} : a(x), b(x) \in \mathbb{Z}_p[x], b(x) \neq 0 \right\}. \bullet$$

Утв. 6. Если характеристика поля отлична от 0, то она является простым числом.

Доказательство следует из того, что если бы характеристика поля была составным числом, то в поле были бы делители нуля. ◁

Утв. 7. Если подполе поля P имеет характеристику p, то и поле P имеет ту же характеристику, и все подполя поля P имеют ту же характеристику.

Доказательство следует из единственности нейтрального элемента в группе и, следовательно, из единственности единицы в любом поле. ◁

Т 5 (о существовании и единственности конечного поля) [Мур, 1893]. Для каждого простого числа p и любого натурального числа n существует конечное поле $\mathbb{F}_q$ из $q = p^n$ элементов. Поле $\mathbb{F}_q$ единственно с точностью до изоморфизма.

Замечание. Поле $\mathbb{F}_q$ с $q = p^n$ обозначают также $\mathbb{F}_p^n$.

Элиаким Гастингс Мур
(англ. *Eliakim Hastings Moore*)
(1862–1932)
американский математик.
С момента открытия в 1892 г. Чикагского университета возглавлял там факультет математики в течение почти 40 лет. Этот факультет стал вторым факультетом в США (после университета Джона Хопкинса), на котором велись исследования в области математики.
Американское математическое общество учредило премию в его честь.

W W W W W W W W W W W W W W W W W W W W W W W W W W W W W W W W W W

Следствие. Поле $\mathbb{F}_p^n$ изоморфно полю $\mathbb{Z}_p[x]/(m(x))$ для любого неприводимого полинома $m(x)$ степени n из кольца $\mathbb{Z}_p[x]$.

Свойства конечных полей

Всякое конечное поле F:

– имеет простую характеристику $p > 1$;

– содержит простое (т. е. не содержащее нетривиальных подполей) подполе $\mathbb{F}_p$ из p элементов, изоморфное полю $\mathbb{Z}_p$;

– содержит $q = p^n$ элементов для некоторого натурального n;

– изоморфно полю $\mathbb{Z}_p[x]/(m(x))$ для любого неприводимого над $\mathbb{Z}_p$ полинома $m(x)$ степени n.

Т 6. Мультипликативная группа конечного поля – циклическая.

Применение в криптографии

Арифметика полей Галуа широко используется в криптографии. В поле Галуа работает вся теория чисел, это поле содержит числа ограниченного размера, при делении отсутствуют ошибки округления. Многие криптосистемы основаны на $\mathrm{GF}(p)$, где p – большое простое число.

Особую роль в приложениях играют поля характеристики 2, в основном из-за простоты выполнения арифметических операций в этих полях. Вычисления в $\mathrm{GF}(2^n)$ могут быть быстро реализованы аппаратно с помощью сдви-

говых регистров с линейной обратной связью. По этой причине вычисления над $\mathrm{GF}(2^n)$ часто быстрее, чем вычисления над $\mathrm{GF}(p)$.

Кроме того, для работы с цифровыми данными естественно использовать $p = 2$ в качестве характеристики поля, поскольку положительные целые числа сохраняются в компьютере как k-битовые слова, в которых k является степенью числа 2 (8, 16, 32, 64 и т. д.). Это означает, что диапазон положительных целых чисел – от 0 до $2^n - 1$.

Соответствие между строками бит и многочленами из поля $\mathrm{GF}(2^n) = \mathbb{Z}_2[x] / (m(x))$, где $m(x)$ – неприводимый многочлен степени n над полем $\mathbb{Z}_2$, описывается следующей схемой.

$$1 \quad 0 \quad 0 \quad 1 \quad 1 \quad 0 \quad 0 \quad 1$$

$$\Updownarrow$$

$$1x^7 + 0x^6 + 0x^5 + 1x^4 + 1x^3 + 0x^2 + 0x^1 + 1x^0$$

$$\Updownarrow$$

$$x^7 + x^4 + x^3 + 1$$

Для поля Галуа $\mathrm{GF}(2^n)$ в криптографии часто используют в качестве модулей трехчлены $m(x) = x^n + x + 1$, так как длинная строка нулей между коэффициентами при x^n и x позволяет просто реализовать быстрое умножение по модулю.