1.1 ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ

В основе современной криптографии лежит *теория чисел*.

Теория чисел или *высшая арифметика* – раздел математики, изучающий натуральные числа и иные похожие величины. В зависимости от используемых методов в теории чисел рассматривают несколько направлений. Нас будут интересовать вопросы *делимости целых чисел*, *вычисления наибольшего общего делителя* (НОД), *разложение числа на простые множители*, *малая теорема Ферма́*, *теорема Эйлера*, элементы *теории вычетов*.

1.1.1 Основные понятия и определения

Определение 1. Множество всех *целых чисел* (обозначим буквой ***Z***) есть набор всех *действительных чисел* без дробной части: {..., -3, -2, -1, 0, 1, 2, 3, ...}.

Определение 2. *Натуральные числа* являются подмножеством целых чисел и образуют множество ***N***: {1, 2, 3, ...}.

Определение 3. *Делимость* – одно из основных понятий теории чисел. Если для некоторого целого числа a и натурального числа b существует целое число q, такое, что $bq=a$, то говорят, что число a *делится* на b. В этом случае b называется *делителем* числа a, а a называется *кратным* числа b. При этом используются следующие обозначения:

$a \vdots b$ – a делится на b или $b \mid a$ – b делит a.

Из последнего определения следует, что:

- любое натуральное число является делителем нуля;
- единица является делителем любого целого числа;
- любое натуральное число является делителем самого себя.

Определение 4. Делитель a называется *собственным делителем* числа b, если $1<|a|<|b|$, и *несобственным* – в противном случае.

Пример 1. $4 \mid 20$; число 4 делит число 20, так как $20 = 4 \cdot 5$. При этом число 4 является собственным делителем числа 20.

Свойство 1 собственного делителя. Положительный наименьший собственный делитель составного числа n не превосходит $\sqrt{n}$.

Определение 5. Всякое целое число a можно представить с помощью положительного целого числа b равенством вида $a = bq + r$, $0 \le r \le b$. Число q называется *неполным частным*, а число r – *остатком* от деления a на b.

1.1.2 Простые и составные числа

Каждое натуральное число, большее единицы, делится, по крайней мере, на два числа: на 1 и на само себя.

Если число не имеет делителей, кроме самого себя и единицы, то оно называется *простым*, а если у числа есть еще делители, то *составным*.

Определение 6. Натуральное число n называется *простым*, если $n > 1$ и не

имеет положительных делителей, отличных от 1 и n.

Простое число не делится без остатка ни на одно другое число.

Пример 2. Первые 10 простых чисел: 2, 3, 5, 7, 11, 13, 17, 19, 23 и 29. Простыми также являются числа 73, 2521, 2365347734339, 2756839 – 1. Количество простых чисел бесконечно велико.

Перечислим несколько ***важных свойств простых чисел***.

Свойство 1. Любое составное число представляется уникальным образом в виде произведения простых чисел; иначе еще говорят, что *разложение числа на простые множители однозначно*.

Это свойство вытекает из основной теоремы арифметики.

Основная теорема арифметики. Всякое натуральное число n, кроме 1, можно представить как произведение простых множителей:

$$n = p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_z,\ z > 1. \qquad (1.1)$$

Пример 3. Целое число 1554985071 = 3·3·4463 ·38713 – произведение четырех простых чисел, два из которых совпадают.

Пример 4. Целое число 39616304 = 2·13·7·2·23·13·2·13·2·7 = = 2·2·2·2·7·7·13·13·13·23.

Порядок записи сомножителей после последнего знака равенства соответствует *канонической форме*.

Для того, чтобы представить относительно небольшое число в виде простых сомножителей, достаточно уметь делить числа столбиком. Однако при этом следует придерживаться некоторых простых правил. Для первого деления нужно выбрать наименьшее простое число большее 1, которое делит исходное число без остатка. Частное от первого деления также нужно разделить с учетом указанных ограничений. Процесс деления продолжаем до тех пор, пока частным не будет 1. Рассмотрим это на примерах.

Пример 5. Представить числа 144 и 39616304 в виде простых сомножителей. Порядок действий виден из нижеследующей иллюстрации.

144	2	1-й шаг	39616304	2
72	2	2-й шаг	19808152	2
36	2		9904076	2
18	2	…..	4952038	2
9	3		2476019	7
3	3		353717	13
1			27209	7
			3887	13
			299	13
			23	23
			1	

Таким образом, 144 = 2·2·2·2·3·3. Результат операций над другим числом был представлен выше в примере 4.

Свойство 2. Простых чисел бесконечно много, причем существует примерно $n/\ln(n)$ простых чисел, меньших числа n.

Свойство 3. *Наименьший простой делитель* составного числа n не

превышает $\sqrt{n}$, поэтому *для проверки простоты числа* достаточно проверить его делимость на 2 и на все нечетные (а еще лучше простые) числа, не превосходящие $\sqrt{n}$; как видим, данное свойство коррелирует со свойством 1 собственного делителя.

Из соотношения $n=qp$ натуральных чисел, больших единицы, следует, что либо p, либо q принадлежит отрезку от 2 до $\sqrt{n}$.

Поиск сомножителей числа n может вестись, например, перебором всех простых чисел до $\sqrt{n}$. Однако, если множители – большие простые числа, то на их поиск может потребоваться много времени.

Сложность решения задачи разложения *больших чисел на простые сомножители, известной как проблема факторизации*, определяет криптостойкость некоторых алгоритмов асимметричной криптографии, в частности алгоритма RSA.

Свойство 4. Любое четное число, большее 2, представимо в виде суммы двух простых чисел, а любое нечетное, большее чем 5, представимо в виде суммы трех простых чисел.

Свойство 5. Для любого натурального n, большего 1, существует хотя бы одно простое число на интервале от n до $2n$.

Определение 7. Натуральное число n называется составным, если $n > 1$ и имеет, по крайней мере, один положительный делитель, отличный от 1 и n.

Единица не считается ни простым числом, ни составным.

Пример 6. Числа 17, 31 – простые, а числа 14, 15 — составные (14 делится на 2 и на 7, 15 делится на 3 и на 5).

Вернемся к собственному делителю.

Свойство 2 собственного делителя. Положительный наименьший собственный делитель составного числа n есть *простое число*.

Так как простое число не делится ни на какое другое, кроме себя самого, очевидный способ проверки числа n на простоту – разделить n на все числа n-1 и проанализировать наличие остатка от деления. Этот способ «в лоб» часто реализуется в компьютерных программах. Однако перебор может оказаться достаточно трудоемким, если на простоту нужно проверить число с количеством цифр в несколько десятков.

Существует правила, способные заметно сократить время вычислений [3].

Правило 1. Воспользоваться свойством 3 простых чисел (см. выше).

Пример 7. Проверим, является ли число 287 простым числом? Для этого найдем наименьший собственный делитель этого числа:

проверяем все простые числа от 2 до$\sqrt{287}$, т. е. от 2 до 13 (берется наибольшее простое число, не превышающее значение корня квадратного; $\sqrt{287}\approx16{,}94$).

получаем: ни одно из вышеуказанных простых чисел не является делителем числа 287. Таким образом, число 287 является простым.

Правило 2. Если последняя цифра анализируемого числа является четной, то это число заведомо составное.

Правило 3. Числа, делящиеся на 5, всегда оканчиваются пятеркой или нулем. Если младшим разрядом анализируемого числа являются 5 или 0, то

такое число не является простым.

Правило 4. Если анализируемое число делится на 3, то и сумма его цифр тоже обязательно делится на 3.

Пример 8. Анализируемое число: 136827658235479371. Сумма цифр этого числа равна: 1 + 3 + 6 + 8 + 2 + 7 + 6 + 5 + 8 + 2 + 3 + 5 + 4 + 7 + 9 + 3 + 7 + 1 = 87. Это число делится на 3 без остатка: 87 = 29·3. Следовательно, и наше число тоже делится на 3 и является составным.

Правило 5. Основано на свойстве делимости на 11. Нужно из суммы всех нечетных цифр числа вычесть сумму всех четных его цифр. Четность и нечетность определяется счетом от младшего разряда. Если получившаяся разность делится на 11, то и анализируемое число тоже на него делится.

Пример 9. Анализируемое число: 2576562845756365782383. Сумма его четных цифр равна: 8 + 2 + 7 + 6 + 6 + 7 + 4 + 2 + 5 + 7 + 2 = 56. Сумма нечетных: 3 + 3 + 8 + 5 + 3 + 5 + 5 + 8 + 6 + 6 + 5 = 57. Разность между ними равна 1. Это число не делится на 11, а следовательно, 11 не является делителем анализируемого числа.

Правило 6. Основано на с*войстве делимости на 7 и 13*. Нужно разбить анализируемое число на тройки цифр, начиная с младших разрядов. Просуммировать числа, стоящие на нечетных позициях, и вычесть из них сумму чисел на четных. Проверить делимость результата на числа 7 и 13.

Пример 10. Анализируемое число: 2576562845756365782383. Перепишем его так: 2 576 562 845 756 365 782 383. Просуммируем числа, стоящие на нечетных позициях, и вычтем из них сумму чисел на четных: (383 + 365 + 845 + 576) - (782 + 756 + 562 + 2) = 67. Это число не делится ни на 7, ни на 13, а значит и делителями заданного числа они не являются.

Определение 8. Если два простых числа отличаются на 2, то их называют *числами-близнецами*.

Таких чисел не очень много. Например, ими являются 5 и 7, 29 и 31, 149 и 151.

Всякое натуральное число $n > 1$либо является простым числом, либо имеет простой делитель.

Воспользуемся перечисленными свойствами для определения простоты числа 2009. Это число не делится на 2 (так как оно нечетно), не делится также на 3 (сумма его цифр 2+9=11 не делится на 3), не делится и на 5. Воспользуемся далее свойством 6: попробуем разделить 2009 на 7; в результате получается целый результат: 287. Таким образом, получен ответ: число 2009 – составное.

Понятно, что в криптографии используются числа, проверка на простоту которых производится гораздо дольше, и для работы с этими числами требуются специальные программные средства. К вопросу проверки чисел на простоту мы еще вернемся. Здесь же отметим, что первый *алгоритм нахождения простых* чисел, не превышающих *n,* был придуман Эратосфеном во 2 в. до н. э. и известен сейчас как «*решето Эратосфена*». Его суть в последовательном исключении из списка целых чисел от 1 до *n* чисел (или из сокращенного диапазона, например, от *m* до *n,* $1<m\leq n$), кратных 2, 3, 5 и

другим простым числам, уже найденным «решетом». Как видим, описанное выше свойство 2 простых чисел и положено в основу рассматриваемого алгоритма.

Для нахождения всех простых чисел не больше заданного числа n в соответствии с «*решетом Эратосфена*» нужно выполнить следующие шаги:

1. Выписать подряд все целые числа от двух (либо от m) до n (2, 3, 4, …, n).

Пусть некоторая переменная (положим s) изначально равна 2 – первому простому числу.

2. Удалить из списка числа от 2s до n, считая шагами по s (это будут числа кратные s: 2s, 3s, 4s, …).

3. Найти первое из оставшихся чисел в списке, большее чем s, и присвоить значению переменной s это число.

4. Повторять шаги 2 и 3, пока возможно.

Пример 11. Примем n =15.

Шаг 1. Выпишем числа от 2 до 15:

2, 3, 4, 5, 6, 7, 8, 9, 10, 10, 11, 12, 13, 14,15.

Шаг 2. Удалим из списка числа с учетом s=2:

2, 3, 5, 7, 9, 11, 13,15. В этом списке первое число, большее, чем s=2, это 3. Текущему s присваивается новое значение: s =3.

Шаг 3. Удалим из списка числа с учетом s=3:

2, 3, 5, 7, 11, 13, 15. В этом списке первое число, большее, чем s=3, это 5.

Текущему s присваивается новое значение: s =5.

Шаг 4. Удалим из списка числа с учетом s=5:

2, 3, 5, 7, 13. В этом списке первое число, большее, чем s=5, это 7. Однако, в этом списке уже нет чисел, кратных текущему значению s, т.е. 7.

Таким образом, числа 2, 3, 5, 7, 13 являются простыми в диапазоне от 1 до 15. Как видим, количество таких чисел – 5.

Вспомним Свойство 2 *простых чисел* и посмотрим, как оно «работает» для нашего примера. Вычислим $n/\ln(n)$ = 15/ ln15 ≈ 5,5. Результат (с учетом округления до целого) близок к истинному: количеству простых чисел от 1 до n =15.

Пример 12. Найти все простые числа из промежутка [800; 830].

Воспользуемся Свойством 3 простых чисел и вычислим $\sqrt{830} \approx 28{,}8$, т. е. меньше 29. Запишем числа из заданного диапазона и удалим последовательно все числа, делящиеся на простые числа от 2 до 28. Такими простыми числами являются: 2, 3, 5, 7, 11, 13, 17,19, 23. После выполнения всех операций в «решете» останутся числа: 809, 811, 821, 823.

Помимо рассмотренного алгоритма Эратосфена, который, понятно, является наименее эффективным, в настоящее время разработаны и используются другие алгоритмы. Описание и программную реализацию этих алгоритмов, можно найти, например, в известной и популярной у разработчиков криптографических приложений книге [4].

1.1.3 Взаимно простые числа и φ-функция

Понятие *делимости чисел* (см. Определение 3) является одним из важных в теории чисел. С этим понятием, а также с его производным – *общим делителем* (Определение 4) связаны другие важнейшие (в частности, для криптографии) понятия: *наибольшего общего делителя* (НОД) и *взаимно простых чисел*.

Определение 9. Наибольшее целое число, которое делит без остатка числа a и b называется *наибольшим общим делителем* этих чисел, *НОД* (a, b).

Пример 13. Делителями числа a=24 являются: 1, 2, 4, 6, 8, 12, 24; делителями числа b=32 являются: 1, 2, 4, 8, 16, 32. Как видим, НОД (24, 32) = 8.

Понятно, что значение НОД можно вычислять для неограниченного ряда чисел.

Простым и эффективным средством вычисления НОД (a, b) является метод или *алгоритм Евклида* (примеры его использования приведены в [2]. В основе алгоритма лежит Определение 5. В соответствии с этим определением используется цепочка вычислений двумя исходными (начальными) числами: a и b:

$$a_i = b_i q_i + r_i, \ 0 \le r_i \le b_i. \qquad (1.2)$$

При $i = 0$ в (1.2) a_i и b_i соответствуют как раз числам a и b. Последний ненулевой остаток (r_i, $i \ge 0$) соответствует НОД (a, b).

Пример 14. Пусть $a = 1234$, $b = 54$. Найти НОД.

$$1234 = 54 \cdot 22 + 46;$$
$$54 = 46 \cdot 1 + 8;$$
$$46 = 8 \cdot 5 + 6;$$
$$8 = 6 \cdot 1 + \mathbf{2};$$
$$6 = 2 \cdot 3 + 0.$$

Последний ненулевой остаток равен 2, поэтому НОД (1234, 54) = 2.

Чтобы найти НОД нескольких чисел (например, a, b, c), достаточно найти НОД двух чисел (например, НОД(a, b) = d) потом НОД полученного (НОД(a, b)) и следующего числа (НОД(c, d) и т. д.

Таким образом, чтобы вычислить НОД k чисел, нужно последовательно вычислить (k–1) НОД. Последнее вычисление дает искомый результат.

Определение 10. *Взаимно простыми* являются целые числа, наибольший общий делитель которых равен 1.

Пример 15. Взаимно простыми являются числа 11 и 7, 11 и 4, хотя число 4 само по себе не является простым.

Теорема 1. Целые числа a и b взаимно просты тогда и только тогда, когда существуют такие целые u и v, что выполняется равенство

$$au + bv = 1. \qquad (1.3)$$

Теорема 2. Если НОД (a, b) = d , то справедливо следующее соотношение (*соотношение Безу*):

$$au + bv = d. \qquad (1.4)$$

Формула (1.4) называется также реализацией «*расширенного алгоритма Евклида*». Этот алгоритм состоит из двух этапов: собственно алгоритма Евклида и вычислений на основе обратных подстановок или последовательного выражения остатков в каждом из шагов предыдущего этапа с соответствующим приведением подобных на каждом шаге.

Пример 16. Для демонстрации обратимся к примеру 14, который составляет первый из указанных этапов. Ниже приведена таблица, из которой можно легко понять, как по алгоритму Евклида вычисляются остатки:

$1234 = 54 \cdot 22 + 46$	$46 = 1234 - 54 \cdot 22$
$54 = 46 \cdot 1 + 8$	$8 = 54 - 46 \cdot 1$
$46 = 8 \cdot 5 + 6$	$6 = 46 - 8 \cdot 5$
$8 = 6 \cdot 1 + 2$	$2 = 8 - 6 \cdot 1$

Обратные подстановки или проход вверх начинаются от записи равенства в нижней строке правого столбца таблицы: $2 = 8 - 6 \cdot 1$. Далее вместо цифры 6 подставляется ее значение из равенства строкой выше: $2 = 8 - (46 - 8 \cdot 5) \cdot 1$ и т. д. Полная цепочка подстановок и преобразований выглядит так:
$2 = 8–(46–8·5)·1 = 8–46+8·5 = 8·6–46 = (54–46)·6–46 = 54·6–46·6–46 = 54·6 – – 46·7 = 54·6–(1234–54·22) ·7 = 54·6–1234·7+54·154 =$ **$54 \cdot 160+(-7) \cdot 1234$** $=$ 8640—8638. Из выражения перед последним знаком равенства (выделено) следует, что для нашего примера $u = -7$ и $v = 160$ в соответствии с формой записи в (1.4).

Исследованием целых чисел занимался швейцарский математик Леонард Эйлер (Leonard Euler). Один из важных вопросов его исследования: сколько существует натуральных чисел, не превосходящих некоторое число n и взаимно простых с n? Ответ на этот вопрос связан с каноническим разложением числа n на простые множители (см. выше основную теорему арифметики и пример 4). Так, если

$$n = p_1^{a_1} \times p_2^{a_2} \times \cdots \times p_n^{a_n} \qquad (1.5)$$

где $p_1, p_2, ..., p_n$ – разные простые множители, то число $\varphi(n)$ натуральных чисел, не превосходящих n и взаимно простых с n можно точно определить по формуле

$$\varphi(n) = n \times \left(1 - \frac{1}{p_1}\right) \times \left(1 - \frac{1}{p_2}\right) \times \cdots \times \left(1 - \frac{1}{p_n}\right) \qquad (1.6)$$

Число натуральных чисел, не превосходящих n и, взаимно простых с n, называется *функцией Эйлера* и обозначается $\varphi(n)$.

Пример 16. Определить количество натуральных чисел, не превосходящих 12 и взаимно простых с 12.

Взаимно простыми с 12 будут четыре числа 1, 5, 7, 11, т. е. $\varphi(12) = 4$ – получено методом «ручного» подсчета.

Теперь подсчитаем $\varphi(12)$ по (1.5). Вспомнив примеры 4 и 5, запишем каноническое разложение числа 12: $12 = 2 \cdot 2 \cdot 3 = 2^2 \cdot 3$, т. е. $p_1 = 2$, $p_2 = 3$. Теперь подсчитаем функцию Эйлера, $\varphi(12)$:

$$\varphi(12) = 12 \cdot (1–1/2) \cdot (1–1/3) = 4.$$

Если p – простое число, то $\varphi(p) = p – 1$, если числа p и q являются простыми и $p \neq q$, то

$$\varphi(p) = (p – 1)(q – 1). \qquad (1.7)$$

1.1.4 Модулярная арифметика и обратные числа по модулю

Понятие «*модулярная арифметика*» ввел немецкий ученый Гаусс. В этой арифметике мы интересуемся остатком от деления числа a на число n (n – натуральное число и $n>1$). Если таким остатком является число b, то можно записать:

$$a \equiv b \pmod{n} \quad \text{или} \quad a \equiv b \bmod n.$$

Такая формальная запись читается как «a сравнимо с b по модулю n».

При целочисленном (в том числе и нулевом) результате деления числа a на число n справедливо $a = b + kn$.

Пример 17. При a=13 и n= 4 имеем b=1, т.е. 13 = 1 + 3·4. Для данного примера справедлив вывод: число 13 по модулю 4 равно 1 или числа 13 и 1 равны по модулю 4.

Пример 18. Справедливы следующие сравнения чисел:

–5≡7 mod 4 ≡11 mod 4 ≡23 mod 4 ≡3 mod 4.

Иногда b называют *вычетом* по модулю n, а числа a и b называют *сравнениями* (по модулю n).

Модулярная арифметика так же *коммутативна*, *ассоциативна* и *дистрибутивна*, как и обычная арифметика. В силу этих свойств сравнения можно почленно складывать, вычитать, умножать, возводить в степень ($a^m \bmod n \equiv (a \bmod n)^m$, если $a \equiv b \bmod n$, то $a^m \equiv b^m \pmod{n}$; другие примеры см. в [2]).

Указанные свойства позволяют упрощать сложность и время выполнения многих вычислений. Криптография использует множество вычислений по модулю n, потому что задачи типа вычисления *дискретных логарифмов* и квадратных корней очень трудны. Кроме того, с вычислениями по модулю удобнее работать, потому что они ограничивают диапазон всех промежуточных величин и результата.

Обратные числа в модулярной арифметике. Традиционно: обратное к 7 равно 7^{-1}=1/7, так как 7·(1/7) =1. В модулярной арифметике запись уравнения в виде

$$ax \equiv 1 \bmod n \qquad (1.8)$$

предусматривает поиск таких значений x и k, которые удовлетворяют равенству

$$ax = nk + 1. \qquad (1.9)$$

Общая задача решения уравнения (1.8) может быть сформулирована следующим образом**:** найти такое x, что

$$1 \equiv ax \bmod n. \qquad (1.10)$$

Уравнение (1.10) имеет единственное решение, если a *и* n – взаимно простые числа, в противном случае – решений нет.

Уравнение (1.10) можно переписать в ином виде:

$$a^{-1} \equiv x \bmod n. \qquad (1.11)$$

Пример 19. *При* a=5 и n=14 получим x=3: $5^{-1} \equiv 3 \bmod 14$, так как $5 \cdot 3 \pmod{14} \equiv 1$.

Если НОД (a, n) =1, то $a^{-1}a \equiv 1 \bmod n$, a^{-1} – число, обратное a по модулю n.

Справедливо также: если

$$x^{-1} \equiv y \bmod n, \text{ то } y^{-1} \equiv x \bmod n. \qquad (1.12)$$

В силу приведенных рассуждений и обоснований (1.12) удовлетворяют такие числа, при которых выполняется равенств

$$xy + kn = 1, \qquad (1.13)$$

где k – целое число (результат деления xy/n).

Нахождение чисел, обратных по модулю, легко реализуется с помощью расширенного алгоритма Евклида (см пример 16 и программную реализацию алгоритма в [2]).

Пример 20. Решить уравнение $7y \equiv 1 \bmod 40$ или $y^{-1} \equiv 7 \bmod 40$

Находим НОД (7,40) – прямая прогонка (алгоритм Евклида):

$40 = 7 \cdot 5 + 5$,

$7 = 5 \cdot 1 + 2$,

$5 = 2 \cdot 2 + 1$, т. е. НОД (7,40) = 1.

Обратная подстановка (приведение (1.12) к форме (1.13):

$1=5–2\cdot2=5–2(7–5\cdot1)=5\cdot3+7(-2)=(40–7\cdot5)3+7(-2) = 40\cdot3+7(-17) = kn + xy=1 \pmod n$, или $7(-17) = 7y$, так как $-17 \bmod 40 = 23$, то y=23: число 23 является обратным числу 7 по модулю 40.

Малая теорема Ферма. Если n – простое число, а число a не кратно n, то справедливо:

$$a^n \equiv 1 \bmod n. \qquad (1.14)$$

В соответствии с *обобщением Эйлера* приведенной теоремы, если НОД (a, n) =1, то справедливо:

$$a^{\varphi(n)} \bmod n \equiv 1. \qquad (1.15)$$

Последнее выражение можно переписать в следующем виде:

$$a^{-1} \bmod n \equiv a^{\varphi(n)-1} \bmod n. \qquad (1.16)$$

Пример 21. Найти число, обратное 5 по модулю 7. Число 7 является простым. Поэтому $\varphi(7) = 7 - 1 = 6$. Теперь с помощью (1.16) получаем: $5^{6-1} \bmod 7 \equiv 5^5 \bmod 7 \equiv 3$.

Таким образом, $5^{-1} \bmod 7 \equiv 3$ или $5 \cdot 3 \equiv 1 \bmod 7$.