Криптографическая защита информации

Лекция 3

Элементы теории чисел

Теория чисел и криптография

Многие результаты теории чисел, как и других фундаментальных наук, долгое время не были очень широко применимы на практике.

Однако с развитием информационных технологий и криптографии теория чисел позволила реализовать ряд прорывных решений, среди которых выделяются криптосистемы с открытым ключом.

Выделим следующие: протоколы согласования ключей, шифры с открытым ключом, игровые протоколы, протоколы электронного голосования, электронные деньги и др.

Некоторые понятия и темы теории чисел

- Простые числа;
- Делимость, остаток от деления;
- Наибольший общий делитель;
- Наименьшее общее кратное;
- Разложение чисел на простые множители;
- Проверка чисел на простоту;
- Генерация больших простых чисел;
- Взаимно простые числа;
- Функция Эйлера;
- Теоремы Эйлера и Ферма;
- …

Остаток от деления одного числа на другое

Пусть даны натуральные числа ***a*** и ***b***, тогда число ***r*** из диапазона $0 \le r < b$ называется остатком от деления числа ***a*** на число ***b***, если существует целое число ***k***, при котором выполняется равенство $a = k*b + r$. Говорят также, что ***k*** – это результат деления нацело (целая часть) числа ***a*** на число ***b***.

Примеры.

27 = 3*9 + 0 => 27 mod 9 = 0 и ***27 div 9 = 3***;

45 = 4*11 + 1 => 45 mod 11 = 1 и ***45 div 11 = 4***;

17 = 3*5 + 2 => 17 mod 5 = 2 и ***17 div 5 = 3***.

*Если остаток от деления одного числа на другое равен **0**, то говорят, что первое число **делится** на второе.*

Простое число

Целое положительное число называется ***простым***, если оно делится только на ***1*** и на само себя.

Целое положительное число называется ***составным***, если у него существует хотя бы один делитель, отличный от ***1*** и его самого.

Примеры.

2, 3, 5, 7, 11, 13, 17 – это простые числа.

15, 30, 45, 100 – это составные числа.

Количество простых чисел

Утверждение. Количество простых чисел, не превосходящих ***n***, примерно равно ***n/ln(n)***.

Более точно.

Количество простых чисел, не превосходящих n, лежит в промежутке от

0,921*n/ln(n) до ***1,106* n/ln(n)***.

N	Нижняя граница	Верхняя граница
100	19	24
1 тыс.	133	160
10 тыс.	999	1200
100 тыс.	7999	9606
1 млн.	66664	80054

Как проверить, является ли число простым?

Самый очевидный алгоритм.

Алгоритм. Вход число ***n***.

```
Цикл i От 2 До n-1
   Начало цикла
      Если n делится на i, Тогда
         Ответ – false (не простое)
   Конец цикла
Ответ – true (простое)
```

«Решето Эратосфена» (алгоритм поиска простых чисел)

Дано: число ***N***.

Найти: все простые числа < ***N***.

Алгоритм:

Выписываем числа ***1, 2, … N-1***;

Вычеркиваем кратные ***2 от 2^2 до N-1***;

Вычеркиваем кратные ***3 от 3^2 до N-1***;

Вычеркиваем кратные ***5 от 5^2 до N-1***;

Вычеркиваем кратные ***7 от 7^2 до N-1***;

……. и так далее до $N^{1/2}$.

«Решето Эратосфена» (пример)

Найдем простые числа, меньшие 61.

1, 2, 3, 4, 5, 6, 7, 8, 9, 10,
11, 12, 13, 14, 15, 16, 17, 18, 19, 20,
21, 22, 23, 24, 25, 26, 27, 28, 29, 30,
31, 32, 33, 34, 35, 36, 37, 38, 39, 40,
41, 42, 43, 44, 45, 46, 47, 48, 49, 50,
51, 52, 53, 54, 55, 56, 57, 58, 59, 60.

Критерий простоты Вильсона

Теорема. Число n является простым тогда и только тогда, когда $(n-1)! = -1 \bmod n$.

Примеры.

$(2-1)! = 1! = 1 = -1 \bmod 2;$

$(3-1)! = 2! = 2 = -1 \bmod 3;$

$(5-1)! = 4! = 24 = -1 \bmod 5;$

$(7-1)! = 6! = 720 = -1 \bmod 7.$

Замечание. Критерий Вильсона бывает удобен при доказательствах, но применять его для проверки простоты невозможно из-за ограмной трудоемкости.

Малая теорема Ферма

Теорема (Ферма). Пусть p – простое, и $0<a<p$. Тогда $a^{p-1} \bmod p = 1$.

Примеры.

$2^{12} \bmod 13 = 1$, $3^{16} \bmod 17 = 1$.

Следствие из теоремы Ферма. Если $a^{p-1} \bmod p \neq 1$

хотя бы для одного числа a из интервала $0<a<p$, то число n – составное.

Определение. Число n называется ***псевдопростым по основанию*** a, если $a^{n-1} \bmod n = 1$.

Тест на простоту на основе малой теоремы Ферма

Требуется проверить, является ли число n простым.

Алгоритм.

Выбираем случайно число a из интервала $0<a<n$ и проверяем условие $a^{n-1} \bmod n = 1$. Если это условие не выполняется, то n – составное.

Если условие выполняется, то n – «вероятно» простое.

Повторив тест еще несколько раз, мы увеличиваем нашу уверенность в простоте числа.

Проблема теста Ферма

Существуют числа, которые являются псевдопростыми по одним основаниям, но не псевдопростыми по другим.

Существуют также числа, которые являются псевдопростыми по всем основаниям.

Такие числа называются ***псевдопростыми*** (без указания основания) или ***числами Кармайкла***.

Количество чисел Кармайкла, не превосходящих ***25 млрд.*** всего ***2163***.

Чисел Кармайкла, не превосходящих ***100000*** всего ***16***: ***561***, ***1105***, ***1729***, ***2465***, ***2821***, ***6601***, ***8911*** и т.д.

Основная теорема арифметики

Теорема. Любое целое положительное число может быть представлено в виде произведения простых чисел, причем единственным образом (с точностью до порядка сомножителей).

Примеры.

$64 = 2^6$.

$100 = 2^2 * 5^2$.

$17 = 17$.

$55 = 5 * 11$.

$30 = 2 * 3 * 5$.

Взаимно простые числа

Два числа называются взаимно простыми, если у них нет общих делителей, кроме ***1***.

Примеры.

Пары взаимно простых чисел: (15,8), (2,3), (100, 99), (1000,3), (45,17).

Пары не взаимно простых чисел: (3,15), (100,20), (30,40), (28,35).

Свойство. Простое число является взаимно простым с любым меньшим него числом.

Пример. Число 11 взаимно просто с числами от 2 до 10.

Функция Эйлера

Пусть дано целое положительное число ***N***. Значение функции Эйлера ***φ(N)*** равно количеству чисел среди ***1,2,3,…,N-1***, которые взаимно просты с ***N***.

Пример.

Вычислим ***φ(15)***.

15 = 3*5.

1, 2, ~~3~~, 4, ~~5~~, ~~6~~, 7, 8, ~~9~~, ~~10~~, 11, ~~12~~, 13, 14.

φ(15) = 8.

Свойство функции Эйлера - 1

Утверждение. Если p - простое, то $\varphi(p) = p-1$.

Доказательство. Поскольку число p – простое, то у него нет делителей, кроме 1 и p.

Следовательно, p может быть не взаимно простым только с теми числами, среди делителей который имеется p.

Очевидно, что любое такое число должно быть больше либо равно p.

Таким образом, в ряду от 1 до $p-1$ таких чисел нет, значит, $\varphi(p)$ равно количеству чисел в этом ряду – из всего $p-1$. ■

Свойство функции Эйлера - 2

Утверждение. Пусть p и q – это простые и $p \neq q$, тогда $\varphi(pq) = (p-1)(q-1)$.

Доказательство. Обозначим $N=pq$. Числа, которые не взаимно просты с N – это те, среди делителей которых есть p или q. Выпишем их:

Делятся на p: p, $2p$, $3p$, $4p$, … , $(q-1)p$.

Делятся на q: q, $2q$, $3q$, $4q$, … , $(p-1)q$.

В первом ряду $q-1$ чисел, а во втором – $p-1$.

Следовательно, $\varphi(N) = (N-1) - ((q-1)+(p-1)) = (p-1)(q-1)$. ■

Две теоремы

Теорема (Эйлер). Если a и b взаимно просты, то $a^{\varphi(b)} = 1 \bmod b$.

Теорема. Если p и q – простые и не равны друг другу, то для произвольного целого k выполняется $a^{k\varphi(pq)+1} = a \bmod pq$.

Наибольший общий делитель

Наибольший общий делитель чисел ***a*** и ***b*** – это наибольшее из всех чисел, которые делят и ***a***, и ***b***.

Обозначение.

НОД(a,b) или ***GCD(a,b)***.

Англ. – Greatest common divisor.

Примеры.

НОД(100,10) = 10; НОД(45,27) = 9;

НОД(100,99) = 1; НОД(17,30) = 1.

Числа являются взаимно простыми тогда и только тогда, когда их наибольший общий делитель равен ***1***.

Наименьшее общее кратное

Наименьшим общим кратным двух чисел называется наименьшее число из всех, которые делятся на оба этих числа.

Вычисление НОК

НОК(a,b) = a*b/НОД(a,b).

Примеры

НОК(6,9) = 6*9/3 = 18;

НОК(10,100) = 10*100/10 = 100;

НОК(24,18) = 24*18/6 = 72.

Вычисление НОД (наивный медленный алгоритм)

Алгоритм. Вход a и b.

```
m := min(a,b);
НОД := 1;
Цикл i от 2 до m
   Если i делит a и b Тогда
      НОД := i;
Ответ – НОД;
```

Алгоритм Евклида

Свойство.

НОД(a,b) = НОД(a mod b, b).

НОД(0,a) = a.

Алгоритм. Вход: ***a*** и ***b***, где ***a*≥*b***.

```
Пока b≠0
   t := a mod b;
   a := b;
   b := t;
Ответ - a
```

Алгоритм Евклида (рекурсивный вариант)

```
Функция НОД(a,b)
   m := min(a,b);
   M := max(a,b);
   Если m=0 Тогда
      Ответ – M;
   Иначе
      Ответ НОД(M mod m, m);
```

Пример.

Диофантово уравнение (частный случай)

Теорема. Пусть даны целые положительные числа a и b. Тогда существуют целые (не обязательно положительные) числа x и y, такие, что

$$ax+by = НОД(a,b).$$

Примеры.

a=93, b=53. НОД(93,53)=1 93*4 + 53*(-7) = 1	a=100, b=68. НОД(100,68)=4 100*(-2) + 68*3 = 4

Расширенный (обобщенный алгоритм Евклида)

Вход: Целые положительные числа ***a*** и ***b***, где ***a≥b***.

Выход: ***x***, ***y*** и ***НОД(a,b)***, где ***x*** и ***y*** удовлетворяют рассмотренному диофантову уравнению.

Алгоритм.

Обозначим $U = (u_1, u_2, u_3)$, $V = (v_1, v_2, v_3)$ и $T = (t_1, t_2, t_3)$.

```
U := (a,1,0), V := (b,0,1).
Пока v1≠0
   q := u1 div v1;
   T := (u1 mod v1, u2-qv2, u3-qv3);
   U := V; V := T;
Ответ – u1 = НОД(a,b); u2 = x; u3 = y.
```

Расширенный алгоритм Евклида (пример)

a=93, b=53.

93 1 0

53 0 1

40 1 -1 q=1

13 -1 2 q=1

1 4 -7 q=3

0 -53 93 q=13

НОД(93,53)=1

x=4, y=-7

Проверка:

93*4 + 53*(-7) = 1

Понятие инверсии

Инверсией числа c по модулю m называется такое число $0<d<m$, которое удовлетворяет соотношению

$$cd \bmod m = 1.$$

Обозначение.

Часто используется обозначение $d = c^{-1} \bmod m$.

В этом случае можно записать $cc^{-1} \bmod m = 1$.

Примеры.

$1 = 1 \bmod m$, $28*31 \bmod 51 = 1$, $3*4 \bmod 11 = 1$.

Вычисление инверсии

Дано: Взаимно простые числа c и m.

Найти: $c^{-1} \bmod m$.

По определению инверсии $cc^{-1} \bmod m = 1$. Согласно определению остатка от деления это равенство означает, что существует k, при котором $cc^{-1} = km + 1$ или $cc^{-1} - km = 1$.

Обозначим $a:=m$, $b:=c$, $x:=-k$, $y:=c^{-1}$ и получим диофантово уравнение: $ax + by = НОД(a,b)$.

Таким образом, для вычисления инверсии нужно решить диофантово уравнение при $a:=m$, $b:=c$, *а затем* $c^{-1}:=y$ *или* $c^{-1}:=y+m$, *если* $y<0$.

Вычисление инверсии (пример)

```
c=19, m=68.
68   0
19   1
11  -3  q=3
8    4  q=1
3   -7  q=1
2   18  q=2
1  -25  q=1
0   68  q=2
```

НОД(68,19)=1, $y=-25$, $c^{-1} = 68-25 = 43$

Проверка: $19*43 \bmod 68 = 1$

Литература

Рябко Б.Я., Фионов А.Н.

Глава 2, параграф 2.3.

Черемушкин А.В.

Лекции по арифметическим алгоритмам в криптографии. Глава I и III.

(электронный вариант книги лежит в обменнике).

Задание (стр. 1)

1. Написать функцию, которая принимает в качестве аргумента целое число и возвращает *true*, если число – простое, и *false* – иначе.
2. Написать функцию, которая принимает в качестве аргументов два целых числа и возвращает *true*, если они – взаимно простые, и *false* – иначе.
3. Написать программу, которая принимает в качестве аргумента целое число и выводит на экран его разложение на простые множители в следующем виде: 360 = 2^3 * 3^2 * 5.
4. Написать функцию, которая принимает в качестве аргумента целое число и возвращает значение функции Эйлера от этого числа.

Задание (стр. 2)

1. Написать функцию, которая принимает в качестве аргументов два целых числа и возвращает их наибольший общий делитель.
2. Написать функцию, которая принимает в качестве аргументов два целых числа и возвращает их наименьшее общее кратное.
3. Написать программу, которая принимает в качестве аргументов числа ***a*** и ***b*** и возвращает структуру из трех полей: ***x***, ***y*** и ***НОД(a,b)***, которые являются решением диофантова уравнения с параметрами ***a*** и ***b***.
4. Написать функцию, которая принимает в качестве аргументов взаимно простые числа ***c*** и ***m*** и возвращает инверсию числа ***c*** по модулю ***m***.