**Лабораторная работа 1. ОСНОВЫ ТЕОРИИ ЧИСЕЛ (ред.1)**

**Цель работы**

Закрепить знания, полученные на лекциях дисциплин «Основы криптографии», «Криптографические методы защиты информации» и приобрести навыки вычислений по блоку занятий «Математический базис криптосистем с открытым ключем».

**Используемое программное обеспечение**

Для работы используется программа “Maxima” и дополнительные командные строки для решения каждой из задач. Напомним, что все материалы к лабораторным работам лежат по адресу P:\\ЛабОКОК\<Номер работы>\.

**Задание**

1.Выполнить упражнения по определению делимости чисел, нахождению их наибольшего общего делителя (*gcd(a,b)*) и по нахождению канонического представления *gcd* и обратного элемента при помощи расширенного алгоритма Евклида.

2.Произвести определение конгруэнтности чисел, проверку утверждений теорем Эйлера и Ферма, убедиться в возможности быстрого вычисления возведения в степень и обращения чисел по модулю.

**Порядок**

Установкить пакета программ “Maxima”

1.Перейти к пакету “Maxima”(M), выбрав в нем функцию *integerp.*

Задавшись не менее, чем тремя произвольными пятиразрядными числами *n* и *d* проверить, являются ли числа *d* делителями *n*, используя следующие команды:

*integerp(n/d)*

2. Используя функцию *divisors(n)* в пакете (М) найти делители не менее чем трех пятиразрядных чисел при помощи следующей команды:

*divisors(n)*

divisors(23019);

divisors(67589);

divisors(71331);

**Проверка**

Находим делители для 23019

23019|3

7673|7673

1

Находим делители для 67589

67589|67589

1

Находим делители для 71331

71331|3

23777|13

1829|31

59|59

1

1, 3, 13, 31, 59, 3\*13=39, 3\*31=93, 3\*59=177, 13\*31=403, 13\*59=767, 31\*59=1829, 3\*13\*31=1209, 3\*31\*59=5487, 3\*13\*59=2301, 13\*31\*59=23777, 1\*71331=71331

Убедиться в правильности расчетов “вручную”.

3.Используя функцию gcd(a,b) пакета (М) найти gcd одной пары четырех разрядных чисел и не менее чем четырех пар пятизначных чисел, одна из которых соответствует взаимно простым числам, при помощи следующей команды:

*gcd(a,b)*

a = 9192;

b = 1149;

a = 16844;

b = 34080;

a = 37134;

b = 51072;

a = 30516;

b = 77428;

a = 31611;

b = 15595;

*gcd(9192,1149);*

*gcd(34080,16844);*

*gcd(51072,37134);*

*gcd(77428,30516);*

*gcd(31611,15595);*

**Проверка**

Найти НОД(8888,2404)

8888 = 2404\*3+1676

2404 = 1676\*1+728

1676 = 728\*2+220

728 = 220\*3+68

220 = 68\*3+16

68 = 16\*4+4

16 = 4\*4

НОД(8888,2404)=4

Убедиться в правильности расчетов “вручную” (на бумаге), выполнив следующее задание

Найти наибольший общий делитель для пары чисел.

Четные номера. Найти НОД(8888,24NN),

Нечетные номера. Найти НОД(4848,12(NN+1)),

где NN –двузначный номер по журналу. Например, если номер 29, то второе число 1230.

4. Для найденных в п.3 пяти gcd(a,b), найти их канонические представления при помощи расширенного алгоритма Евклида при помощи следующей команды:

*gcdex(a,b)*

*gcd(9192,1149);*

*gcd(34080,16844);*

*gcd(51072,37134);*

*gcd(77428,30516);*

*gcd(31611,15595);*

**Проверка**

***НОД(9192,1149) = 1149***

*9192 = 1149\*8 + 0*

*1149 = (z1\*1149+z2\*9192)mod9192=z1\*1149mod9192*

*z1 = 1*

*z2 = 0*

***НОД (34080,16844) = 4***

*34080 = 16844\*2+392*

*16844 =392\*42+380*

*392 = 380\*1+12*

*380 = 12\*31+8*

*12 = 8\*1 +4*

*8 = 4\*2 + 0*

*4 = (z1\*16844+z2\*34080) mod34080=z1\*16844 mod34080*

*4 =12 - 8*

*8 = 380 – 12\*31*

*12 = 392 – 380*

*380 = 16844-392\*42*

*392 = 34080-16844\*2*

*380 = 16844 - 392\*42 = 16844 – 42\*(34080-16844\*2) = 85\*16844 - 42 \* 34080*

*12 = 392 – 380 = 34080 – 16844\*2 – (85\*16844 - 42 \* 34080) = 43\*34080 - 87\*16844*

*8 = 380 – 12\*31 = 85\*16844 - 42 \* 34080 – (43\*34080 - 87\*16844)\*31 =*

*= 85\*16844 - 42 \* 34080 – 1333\*34080+2967\*16844 = 2 782\*16844 - 1375\*34080*

*4 = 12 – 8 = 43\*34080 - 87\*16844 – (2 782\*16844 - 1375\*34080) = = 43\*34080 - 87\*16844 – 2 782\*16844 +1375\*34080 = 1418\*34080 - 2869\*16844*

z1 = -2869; z2 = 1418

***НОД (51072,37134) = 6***

*51072 = 37134\*1+13938*

*37134 = 13938\*2+9258*

*13938 = 9258\*1+4680*

*9258 = 4680\*1+4578*

*4680=4578\*1+102*

*4578=102\*44+90*

*102=90\*1+12*

*90=12\*7+6*

*12=6\*2+0*

*6 = (z1\*37134+z2\*51072) mod51072=z1\*37134 mod51072*

*6 = 90 – 12\*7*

*12 = 102 – 90*

*90 = 4578 – 102\*44*

*102 = 4680 – 4578*

*4578 = 9258 – 4680*

*4680 = 13938 – 9258*

*9258 = 37134 – 13938\*2*

*13938 = 51072 – 37134\*1*

*9258 = 37134 – 13938\*2 = 37134 – 2\*(51072 – 37134\*1) = 37134 – 2\*51072 + 2\*37134 = 3\*37134 – 2\*51072*

*4680 = 13938 – 9258 = 51072 – 37134\*1 – (3\*37134 – 2\*51072) = 51072 – 37134\*1 – 3\*37134 + 2\*51072 = 3\*51072 – 4\*37134*

*4578 = 9258 – 4680 = 3\*37134 – 2\*51072 – 3\*51072 + 4\*37134 = 7\*37134 – 5\*51072*

*102 = 4680 – 4578 = 3\*51072 – 4\*37134 – 7\*37134 + 5\*51072 =8\*51072 – 11\*37134*

*90 = 4578 – 102\*44 = 7\*37134 – 5\*51072 – 44\*(8\*51072-11\*37134) = 7\*37134 – 5\*51072 – 352\*51072 +484\*37134 = 491\*37134 – 357\*51072*

*12 = 102 – 90 = 8\*51072 – 11\*37134 – 491\*37134 + 357\*51072 = 365\*51072 – 502\*37134*

*6 = 90 – 12\*7 = 491\*37134 – 357\*51072 – 7\*(365\*51072 – 502\*37134) = 491\*37134 – 357\*51072 – 2555\*51072 + 3514\*37134 = 4005\*37134 – 2912\*51072*

z1 =*4005*; z2 = -*2912*

***НОД (77428,30516) = 4***

*77428 = 30516\*2+16396*

*30516 = 16396\*1+14120*

*16396 = 14120\*1+2276*

*14120 = 2276\*6+464*

*2276 = 464\*4+420*

*464 = 420\*1+44*

*420 = 44\*9+24*

*44 = 24\*1+20*

*24 = 20\*1+4*

*20 = 4\*5+0*

*4 = (z1\*30516+z2\*77428) mod77428=z1\*30516**mod77428*

*4 = 24 – 20*

*20 = 44 – 24*

*24 = 420 – 44\*9*

*44 = 464 – 420*

*420 = 2276 – 464\*4*

*464 = 14120 – 2276\*6*

*2276 = 16396 – 14120*

*14120 = 30516 – 16396*

*16396 = 77428 – 30516\*2*

*14120 = 30516 – 16396 = 30516 – 77428 + 30516\*2 = 3\*30516 – 77428*

*2276 = 16396 – 14120 = 77428 – 30516\*2 – (3\*30516 – 77428) = 77428 – 30516\*2 – 3\*30516 +77428 = 2\*77428 – 5\*30516*

*464 = 14120 – 2276\*6 = 3\*30516 – 77428 – 6\*(2\*77428 – 5\*30516) = 3\*30516 – 77428 –12\*77428 + 30\*30516 = 33\*30516 – 13\*77428*

*420 = 2276 – 464\*4 = 2\*77428 – 5\*30516 – 4\*(33\*30516 – 13\*77428) = 2\*77428 – 5\*30516 – 132\*30516 + 52\*77428 = 54\*77428 – 137\*30516*

*44 = 464 – 420 = 33\*30516 – 13\*77428 – 54\*77428 + 137\*30516 = 170\*30516 – 67\*77428*

*24 = 420 – 44\*9 = 54\*77428 – 137\*30516 – 9\*(170\*30516 – 67\*77428) = 54\*77428 – 137\*30516 – 1530\*30516 + 603\*77428 = 657\*77428 – 1667\*30516*

*20 = 44 – 24 = 170\*30516 – 67\*77428 – 657\*77428 + 1667\*30516 = 1837\*30516 – 724\*77428*

*4 = 24 – 20 = 657\*77428 – 1667\*30516 – 1837\*30516 + 724\*77428 = 1381\*77428 – 3504\*30516*

z1 =-*3504*; z2 = *1381*

***НОД (31611,15595) = 1***

*31611 = 15595\*2+421  
15595 = 421\*37+18  
421 = 18\*23+7  
18 = 7\*2+4  
7 = 4\*1+3  
4 = 3\*1+1  
3 = 1\*3+0*

*1 = (z1\*15595+z2\*31611) mod31611=z1\*15595 mod31611*

*1 = 4 – 3*

*3 = 7 – 4*

*4 = 18 – 7\*2*

*7 = 421 – 18\*23*

*18 = 15595 – 421\*37*

*421 = 31611 – 15595\*2*

*18 = 15595 – 421\*37 = 15595 – 37\*(31611 – 15595\*2) = 75\*15595-37\*31611*

*7 = 421 – 18\*23 = 31611 – 15595\*2 – 23\*(75\*15595 – 37\*31611) = 852\*31611 – 1727\*15595*

*4 = 18 – 7\*2 75\*15595 – 37\*31611 – 2\*(852\*31611 – 1727\*15595) = 3529\*15595 – 1741\*31611*

*3 = 7 – 4 = 852\*31611 – 1727\*15595 – (3529\*15595 – 1741\*31611) = 2593\*31611 – 5256\*15595*

*1 = 4 – 3 = 3529\*15595 – 1741\*31611 – (2593\*31611 – 5256\*15595) = 8785\*15595 – 4334\*31611*

z1 =*8785*; z2 = *-4334*

Проверить правильность канонических представлений для всех случаев.

5. Для одного четырехразрядного числа и не менее чем для четырех произвольно выбранных пятизначных чисел *a* сделать их приведение по модулям произвольных меньших чисел *m* при помощи команды:

*mod(a,m)*

a = 3194

m = 3000

a = 74352

m = 52

a = 30292

m = 302

a = 63416

m = 5654

a = 90082

m = 80001

mod(3194,3000);

mod(74352, 52);

mod(30292, 302);

mod(63416, 5654);

mod(90082, 80001);

Убедиться в правильности расчетов для первого числа “вручную”.

6. Найти мультипликативно обратные элементы к одному двухразрядному числу и не менее чем к четырем 9-ти значным числам *a* по простым двузначным модулям *m* при помощи следующей команды:

*power\_mod(a,-1,m)*

a = 85

m = 17

a = 955134357

m = 23

a = 307621530

m = 37

a = 807987190

m = 79

a = 359718709

m = 97

power\_mod(85,-1,17);

power\_mod(955134357,-1, 23);

power\_mod(307621530,-1, 37);

power\_mod(807987190,-1, 79);

power\_mod(359718709,-1, 97);

Убедиться в правильности расчетов “вручную”, выполнив следующее задание:

Найти обратный элемент к числу *а* по *modb*,

где *a* соответствует числу в таблице 1, порядковый номер которого совпадает с Вашим номером по журналу, *b* с номером большим на 10 порядковый номер числа а.

Например, если NN=29, то a=157 b=211

Таблица1.

23 29 31 37 41 43 47 53 59 61

67 71 73 79 83 89 97 101 103 107

109 113 127 131 137 139 149 151 157 163

167 173 179 181 191 193 197 199 211 223

7.Рассчитать функцию Эйлера для одного двухразрядного числа и не менее чем четырех четырехзначных чисел *m*, используя команду:

*totient(m)*

m = 26

m = 8736

m = 9096

m = 5011

m = 9135

totient(26);

totient(8736);

totient(9096);

totient(5011);

totient(9135);

Убедиться в правильности расчетов для первого числа “вручную”.

8.Для двух пар произвольных четырехзначных, но взаимно простых чисел *a* и *m,* проверить справедливость теоремы Эйлера при помощи следующей команды:

*mod(a^ totient(m),m)*

*a =* 2213

*m =* 1931

*a =* 8641

*m =* 7933

*mod(*2213*^ totient(1931),1931);*

*mod(8641^ totient(7933),7933);*

*1*

*1*

9.Произвести возведение 5-значного произвольного числа *a* в степень произвольного 15-значного числа *b* по произвольному 4-х значному модулю *m*, используя команду:

*power\_mod(a,b,m)*

a = 23904

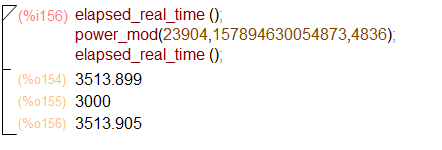
b = 157894630054873

m = 4836

power\_mod(23904,157894630054873,4836);

3000

Убедиться, что возведение в степень выполняется быстрым алгоритмом, а не *b–*кратным перемножением числа *a* самого на себя с приведением по модулю*,* рассчитав примерное время вычислений на данном компьютере при использовании метода перемножения.



Компьютер использует быстрый алгоритм возведения в степень.

Используя алгоритм быстрого возведения в степень, вычислить вручную:

Четные номера. 31NN(mod7).

Нечетные номера. 51NN(mod7).

Например, если номер 3, то показатель степени 103.

10. Решить систему уравнений на основе использования китайской теоремы об остатках.

,

где  заданы таблицей

|  |  |  |
| --- | --- | --- |
| № вар | ai | mi |
| 1 | 3,4,5 | 7,11,19 |
| 2 |  | 5,11,13 |
| 3 |  | 13,7,11 |
| 4 |  | 7,11,13, |
| 5 |  | 11,13,5 |
| 6 | 4,5,6 | 13,19,7 |
| 7 |  | 5,13,17 |
| 8 |  | 17,7,19 |
| 9 |  | 13,5,19 |
| 10 |  | 7,17,13 |
| 11 | 5,7,8 | 5,7,9 |
| 12 |  | 11,13,5 |
| 13 |  | 9,11,13 |
| 14 |  | 7,9,19 |
| 15 |  | 5,11,17 |
| 16 | 3.9,6 | 7,9,11 |
| 17 |  | 11,7,19 |
| 18 |  | 5,17,9 |
| 19 |  | 11,9,13 |
| 20 |  | 7,9,17 |
| 21 | 5,6,7 | 9,13,19 |
| 22 |  | 5,13,11 |
| 23 |  | 7,13,11 |
| 24 |  | 7,9,13, |
| 25 |  | 11,19,7 |

11. Решить контрольный пример.

 , где

k=31, 

*а=№вар+10.*

Примечание. Если получаетcя *b=а, положить b=25.*

**Отчет**

1.Титульный лист.

2.Исходные данные и результаты вычислений по всем 11 пунктам порядка выполнения работы.

3.Подробные вычисления по п. 3, 6, 9, 10,11.

**Контрольные вопросы**

1.Как найти gcd, используя алгоритм Евклида?

2.Как найти обратный элемент по модулю, используя расширенный алгоритм Евклида?

3.Каковы условия существования обратного элемента по модулю некоторого числа?

4.Как производится быстрое возведение в степень с приведением по модулю?

5.Как выполняются, и какими свойствами обладают арифметические действия над сравнениями?

6.Формулировки теорем Эйлера и Ферма.