Лабораторная работа №2

Вариант 13

Кутреева С.И.
872302

① Вычислить НОД(m, n) по алгоритму Евклида

m = 702
n = 1157

НОД(702, 7157) = НОД(1157, 702)

1157 = 702 · 1 + 455
702 = 455 · 1 + 247
455 = 247 · 1 + 208
247 = 208 · 1 + 39
208 = 39 · 5 + 13
39 = 13 · 3 + 0

НОД(702, 1157) = 13

Алгоритм Евклида:
НОД(a,b) = НОД(b, r),
где $a = b \cdot q_1 + r_1$
$b = r_1 \cdot q_2 + r_2$
$r_1 = r_2 \cdot q_3 + r_3$
...
$r_{n-1} = r_n \cdot q_{n+1} + r_{n+1}$
$r_n = r_{n+1} q_{n+2} + 0$
НОД(a,b) = r_{n+1}

② Вычислить НОД(m, n) по бинарному алгоритму

m = 774
n = 1266

По бинарному алгоритму:
1) Если a и b – чётные, то НОД(a,b) = 2НОД(a/2, b/2)
2) Если a – чёт., b – нечёт., то НОД(a,b) = НОД(a/2, b)
3) НОД(a, b) = НОД(b, a-b)
4) Если a и b – нечётные, то (a-b) – чётно

НОД(774, 1266) = НОД(1266, 774) = 2НОД(633, 387) = 2НОД(387, 246) = 2НОД(246, 141) = 2НОД(123, 141) = 2НОД(141, 123) = 2НОД(123, 18) = 2НОД(18, 105) = 2НОД(105, 18) = 2НОД(18, 87) = 2НОД(87, 18) = 2НОД(18, 69) = 2НОД(69, 18) = 2НОД(18, 51) = 2НОД(51, 18) = 2НОД(18, 33) = 2НОД(33, 18) = 2НОД(18, 15) = 2НОД(9, 15) = 2НОД(15, 9) = 2НОД(9, 6) = 2НОД(6, 3) = 2НОД(3, 3) = 2 · 3 = 6.

③ Вычислить функцию Эйлера для n = ...

n = 872

Функция Эйлера (φ(n)):
Если представить n как: $n = p_1^{a_1} \cdot p_2^{a_2} \cdots p_m^{a_m}$, где $p_1, p_2, \ldots, p_m$ – простые числа,
то $\varphi(n) = n \cdot (1 - \frac{1}{p_1}) \cdot (1 - \frac{1}{p_2}) \cdots (1 - \frac{1}{p_m})$.

872	2
436	2
218	2
109	109
1	

$872 = 2^3 \cdot 109^1$

$\varphi(872) = 872 \cdot (1 - \frac{1}{2})(1 - \frac{1}{109}) = \frac{872 \cdot 1 \cdot 108}{2 \cdot 109} = 4 \cdot 108 = \underline{432}$

④ Показать, что $a^b = 1 \bmod n$

$a = 8$
$b = 624$
$n = 689$

Теорема Эйлера:
Если $n \geq 0$ и НОД $(a, n) = 1$, где a – целое, то справедливо $a^{\varphi(n)} = 1 \bmod n$

1) $n = 689 > 0$, при этом $a = 8$ – целое положительное число

2) НОД $(8, 689) =$ НОД $(689, 8) = 1$, т.к по алгоритму Евклида:

$689 = 8 \cdot 86 + 1$
$8 = 1 \cdot 8 + \underline{0}$ $\quad r_{n+1} = 1$

3) $\varphi(689) = 689 \cdot (1 - \frac{1}{13})(1 - \frac{1}{53}) = \frac{689 \cdot 12 \cdot 52}{13 \cdot 53} = 624 = b$

689	13
53	53
1	

Значит, $a^{\varphi(n)} = 1 \bmod n \Rightarrow 8^{624} = 1 \bmod 689$, что соотв-ет $a^b = 1 \bmod n$

⑤ Вычислить взаимообратное число по модулю r для m

$r = 18$
$m = 5$

Взаимообратное по модулю r число n, при этом $(n \cdot m) \bmod r = 1$ или $n \cdot m = 1 \bmod r$. По теореме Эйлера: $n^{\varphi(r)} = 1 \bmod r$ или $1 = n^{\varphi(r)} \bmod r$
Отсюда $n \cdot m = n^{\varphi(r)} \bmod r$ или $m = n^{\varphi(r)-1} \bmod r$

$5n = 1 \bmod 18$

$n = 5^{\varphi(18)-1} \bmod 18 = 5^5 \bmod 18 = 3125 \bmod 18 = \underline{11}$

18	2
9	3
3	3
1	

$18 = 2^1 \cdot 3^2$

$\varphi(18) = 18 \cdot (1 - \frac{1}{2})(1 - \frac{1}{3}) = \frac{18 \cdot 1 \cdot 2}{2 \cdot 3} = 6$

$5 \cdot 11 = 1 \bmod 18 \Rightarrow 55 = 1 \bmod 18$ или $55 \bmod 18 = 1$

⑥ Показать, что $m^n \bmod r = k$

$m = 8, n = 9, r = 17, k = 8$

Модулярная арифметика:
$(a * b) \bmod m = [(a \bmod m) * (b \bmod m)] \bmod m$
где $*$ – вычитание / сложение / умножение

$8^9 \bmod 17 = 8^2 \cdot 8^2 \cdot 8^2 \cdot 8^2 \cdot 8 \bmod 17 =$
$= ((64 \bmod 17)^4 \cdot 8 \bmod 17) \bmod 17 = (13^4 \cdot 8) \bmod 17 = (13^4)^2 8 \bmod 17 = (((169 \bmod 17)^2 8 \bmod 17) \bmod 17 =$
$= (16^2 \cdot 8) \bmod 17 = (2^2 \cdot 8^3) \bmod 17 = (4 \bmod 17 \cdot 512 \bmod 17) \bmod 17 = (4 \cdot 2) \bmod 17 =$
$= 8 \bmod 17 = \underline{8 = k}$