Краткие сведения из теории чисел

1. Наибольший общий делитель (НОД)

Наибольшим общим делителем целых чисел a_1, a_2, …, a_n называется такой положительный общий делитель этих чисел, который делится на любой другой общий делитель этих чисел.

<u>Пример:</u> НОД(21,15)=3 НОД(27,44)=1 НОД(120,66)=6

2. Алгоритм Евклида

Используется для нахождения наибольшего общего делителя двух чисел.

НОД(a, b) = НОД(b, r), где $a = b\cdot q + r$.

<u>Пример:</u> НОД(22, 8) = ?

22 = 8*2 + 6	(22, 8) = (8, 6)
8 = 6*1 + 2	(8, 6) = (6, 2)
6 = 2*2 + 2	(6, 2) = (2, 2)
2 = 2*1 + <u>0</u>	НОД(22, 8) = 2

3. Бинарный алгоритм

Данный алгоритм также используется для нахождения наибольшего общего делителя 2-х чисел и базируется на следующих четырёх утверждениях:

1) Если оба числа a и b – четные, то: НОД(a, b) = 2·НОД(a/2, b/2);
2) Если a – четное, а b – нечетное, то НОД(a, b) = НОД(a/2, b);
3) НОД(a, b) = НОД(b, a– b);
4) если a и b – оба нечетны, то a– b – четно.

<u>Пример:</u> НОД(1173, 323) = ?

(1173, 323) = (323, 850) = (323, 425) = (323, 102) = (323, 51) = (51, 272) = (51, 136) = (51, 68) = (51, 34) = (51, 17) = (17, 34) = (17, 17) = 17

4. Простые числа

Положительное целое не равное нулю число называется простым, если оно делится только на самого себя и на единицу.

<u>Примеры</u>: 11 – простое; 29 – простое; 56 – составное (56 = 7 · 4 · 2).

Два числа M и N называются взаимно простыми, если они не имеют общих делителей кроме единицы, то есть наибольший общий делитель НОД(M, N)=1.

5. Функция Эйлера

Функцией Эйлера $\varphi(n)$ ($n \ge 1$) называют число положительных целых чисел меньших n и взаимно простых с n.

<u>Примеры:</u> $\varphi(1) = 0$ $\varphi(2) = 1$ $\varphi(3) = 2$ $\varphi(4) = 2$ $\varphi(5) = 4$
$\varphi(6) = 2$ $\varphi(7) = 6$ $\varphi(8) = 4$ $\varphi(9) = 6$ $\varphi(10) = 4$ $\varphi(11) = 10$.

Если n – простое число, то $\varphi(n)=n-1$.

Если $n=p\cdot q$, где p и q – простые числа, то $\varphi(n)=(p-1)\cdot(q-1)$.

<u>Пример:</u> $\varphi(35) = \varphi(5) \cdot \varphi(7) = 4 \cdot 6 = 24$.

Обобщенный алгоритм вычисления функции Эйлера для произвольного числа n:

Если n представить как: $n = p_1^{a_1} \cdot p_2^{a_2} \cdot p_3^{a_3} \cdot \ldots \cdot p_r^{a_r}$ (p_1, p_2, …, p_r – простые), то $\varphi(n)=n\cdot(1-1/p_1)\cdot(1-1/p_2)\cdot\ldots\cdot(1-1/p_r)$.

<u>Пример:</u> φ (2700) = ? ($2700=2^2\cdot3^3\cdot5^2$) $\varphi(2700)=2700\cdot(1-1/2)\cdot(1-1/3)\cdot(1-1/5)=720$.

6. Теорема Эйлера

Если $n \ge 0$ – положительное целое число, и (a, n)=1, где a – целое, то справедливо:

$a^{\varphi(n)}=1\ mod\ n$.

7. Взаимобратные числа

Для числа n взаимобратным по модулю r называется такое число m, для которого выполняется $(n \cdot m)$ $mod\ r = 1$ или

$n \cdot m = 1\ mod\ r.$ (1)

По теореме Эйлера: $n^{\varphi(r)}=1\ mod\ r,$ (2)

или $1 = n^{\varphi(r)}\ mod\ r.$ (3)

Перемножив (1) и (3), получим $n \cdot m = n^{\varphi(r)}\ mod\ r$, или $\boldsymbol{m = n^{\varphi(r)-1}\ mod\ r}$

<u>Пример:</u> Найти взаимообратное по модулю 7 для числа 4.

$4 \cdot m = 1\ mod\ 7$, $m = 4^{\varphi(7)-1}\ mod\ 7 = 4^5\ mod\ 7 = \underline{\mathbf{2}}$**,** $4 \cdot 2 = 1\ mod\ 7$.

8. Принципы модулярной арифметики

Модулярная арифметика основывается на следующем равенстве:

$(a*b)\ mod\ m = [(a\ mod\ m)*(b\ mod\ m)]\ mod\ m,$

где * – любая из следующих операций:

«+» (сложение), «–» (вычитание), «×» (умножение).

Данное равенство говорит о том, что вычисление $(a*b)$ $mod\ m$ в модулярной арифметике даёт тот же результат что и вычисление $(a*b)$ в обычной целочисленной арифметике с последующим взятием остатка от деления полученного результата на m (mod m).

<u>Пример:</u> $7 \cdot 9\ mod\ 5 = [(7\ mod\ 5) \cdot (9\ mod\ 5)]\ mod\ 5 = [2 \cdot 4]\ mod\ 5 = 3$.

Принципы модулярной арифметики также применимы к операции возведения в степень, поскольку возведение в степень эквивалентно многократному умножению.

<u>Пример</u>: Вычислим выражение $3^5\ mod\ 7$. $3^5\ mod\ 7 = 3 \cdot 3 \cdot 3 \cdot 3 \cdot 3\ mod\ 7 = 243\ mod\ 7 = 5$.

Возведение 3 в степень 5 и затем взятие результата по модулю 7 может быть произведено следующим образом. Представим $5 = 2 \cdot 2 + 1$, тогда $3^5 = 3^{2 \cdot 2+1} = (3^2)^2 \cdot 3^1$. Затем

1. Возводим число 3 в квадрат и берем по модулю 7:
   $(3^2)^2\ mod\ 7 = 3^2 \cdot 3^2\ mod\ 7 = 2 \cdot 2\ mod\ 7 = 4$.
2. Возводим результат в квадрат и берем по модулю 7:
   $(3^2)^2\ mod\ 7 = 3^2 \cdot 3^2\ mod\ 7 = 2 \cdot 2\ mod\ 7 = 4$.
3. Умножаем полученный результат на 3 и берем по модулю 7:
   $(3^2)^2 \cdot 3\ mod\ 7 = [((3^2)^2\ mod\ 7) \cdot 3]\ mod\ 7 = [4 \cdot 3]\ mod\ 7 = \underline{\mathbf{5}}$.

9. Алгоритм быстрого возведения в степень по модулю

$x = a^z\ mod\ n$

```
function fast_exp(a,z,n)
begin
    a1:=a; z1:=z; x:=1;
    while z1<>0 do
    begin
        while (z1 mod 2)=0 do
        begin
        z1:=z1 div 2;
            a1:=(a1*a1) mod n;
        end;
        z1:=z1-1;
        x:=(x*a1) mod n;
    end;
    fast_exp:=x;
end;
```

Задание по лабораторной работе №2

1. Вычислите НОД (m, n) по алгоритму Евклида.
2. Вычислите НОД(m, n) используя бинарный алгоритм.
3. Вычислите функцию Эйлера для n=… (произвольное число).
4. Покажите, что a^b=1 *mod n*.
5. Вычислите взаимообратное число по модулю *r* для *m*.
6. Покажите, что m^n *mod r* = *k*.

Вариант 1

1. m=347, n=723;
2. m=112, n=679;
3. n=324;
4. a=4, b=336, n=377;
5. r=29, m=5;
6. m=8, n=7, r=13, k=5.

Вариант 2

1. m=2674, n=1699;
2. m=2674, n=1118;
3. n=886;
4. a=7, b=264, n=299;
5. r=18, m=7;
6. m=9, n=7, r=17, k=2.

Вариант 3

1. m=1236, n=935;
2. m=1778, n=994;
3. n=632;
4. a=10, b=220, n=253;
5. r=26, m=5;
6. m=7, n=9, r=17, k=10.

Вариант 4

1. m=845, n=652;
2. m=964, n=1277;
3. n=953;
4. a=14, b=448, n=493;
5. r=55, m=6;
6. m=9, n=8, r=13, k=3.

Вариант 5

1. m=1974, n=528;
2. m=998, n=1285;
3. n=746;
4. a=13, b=504, n=551;
5. r=91, m=8;
6. m=9, n=7, r=19, k=4.

Вариант 6

1. m=933, n=525;
2. m=525, n=1385;
3. n=724;
4. a=12, b=648, n=703;
5. r=26, m=11;
6. m=6, n=12, r=13, k=1.

Вариант 7

1. m=1532, n=643;
2. m=994, n=778;
3. n=488;
4. a=13, b=672, n=731;
5. r=13, m=5;
6. m=4, n=11, r=17, k=13.

Вариант 8

1. m=835, n=1562;
2. m=838, n=1200;
3. n=678;
4. a=8, b=360, n=407;
5. r=33, m=5;
6. m=8, n=9, r=19, k=18.

Вариант 9

1. m=2525, n=1186;
2. m=745, n=1375;
3. n=884;
4. a=15, b=756, n=817;
5. r=44, m=7;
6. m=5, n=9, r=17, k=12.

Вариант 10

1. m=472, n=844;
2. m=844, n=1483;
3. n=625;
4. a=24, b=936, n=1007;
5. r=28, m=7;
6. m=5, n=8, r=19, k=4.

Вариант 11

1. m=552, n=874;
2. m=1934, n=725;
3. n=863;
4. a=6, b=480, n=527;
5. r=23, m=3;
6. m=5, n=8, r=19, k=4.

Вариант 12

1. m=552, n=938;
2. m=938, n=1366;
3. n=728;
4. a=9, b=832, n=901;
5. r=32, m=9;
6. m=6, n=9, r=23, k=16.

Вариант 13

1. m=702, n=1157;
2. m=774, n=1266;
3. n=872;
4. a=8, b=624, n=689;
5. r=18, m=5;
6. m=8, n=9, r=17, k=8.

Вариант 14

1. m=998, n=1285;
2. m=1974, n=528;
3. n=474;
4. a=8, b=624, n=689;
5. r=33, m=5;
6. m=6, n=9, r=23, k=16.

Вариант 15

1. m=1045, n=836;
2. m=686, n=1078;
3. n=842;
4. a=5, b=520, n=583;
5. r=25, m=6;
6. m=5, n=7, r=11, k=3.

Вариант 16

1. m=1934, n=725;
2. m=552, n=874;
3. n=375;
4. a=8, b=624, n=689;
5. r=25, m=6;
6. m=5, n=9, r=11, k=9.

Вариант 17

1. m=1265, n=2024;
2. m=1092, n=689;
3. n=634;
4. a=6, b=312, n=371;
5. r=16, m=3;
6. m=5, n=9, r=11, k=9.

Вариант 18

1. m=1778, n=994;
2. m=1236, n=935;
3. n=552;
4. a=5, b=520, n=583;
5. r=18, m=5;
6. m=6, n=9, r=23, k=16.

Вариант 19

1. m=686, n=1078;
2. m=1045, n=836;
3. n=556;
4. a=8, b=624, n=689;
5. r=32, m=9;
6. m=8, n=9, r=19, k=18.

Вариант 20

1. m=844, n=1483;
2. m=472, n=844;
3. n=423;
4. a=24, b=936, n=1007;
5. r=44, m=7;
6. m=8, n=9, r=19, k=18.

Вариант 21

1. m=1092, n=689;
2. m=1265, n=2024;
3. n=734;
4. a=14, b=448, n=493;
5. r=29, m=5;
6. m=5, n=8, r=19, k=4.

Вариант 22

1. m=1093, n=779;
2. m=1531, n=642;
3. n=423;
4. a=11, b=221, n=153;
5. r=48, m=5;
6. m=5, n=13, r=19, k=23.

Вариант 23

1. m=938, n=1366;
2. m=552, n=938;
3. n=867;
4. a=7, b=264, n=299;
5. r=91, m=8;
6. m=9, n=8, r=13, k=3.

Вариант 24

1. m=994, n=778;
2. m=1532, n=643;
3. n=462;
4. a=6, b=312, n=371;
5. r=44, m=7;
6. m=6, n=9, r=23, k=16.

Вариант 25

1. m=999, n=779;
2. m=1331, n=623;
3. n=662;
4. a=10, b=210, n=291;
5. r=43, m=9;
6. m=8, n=11, r=19, k=13.

Вариант 26

1. m=1021, n=1067;
2. m=553, n=1093;
3. n=678;
4. a=7, b=264, n=299;
5. r=91, m=8;
6. m=9, n=8, r=13, k=3.

Вариант 27

1. m=112, n=679;
2. m=347, n=723;
3. n=532;
4. a=15, b=756, n=817;
5. r=18, m=7;
6. m=5, n=9, r=11, k=9.

Вариант 28

1. m=938, n=1366;
2. m=552, n=938;
3. n=867;
4. a=7, b=264, n=299;
5. r=32, m=9;
6. m=8, n=11, r=19, k=13.