Лабораторная работа №1
«Алгоритм Евклида»

Задание. Вычислить НОД(a, b) при помощи: 1) алгоритма Евклида с делением с остатком; 2) бинарного алгоритма Евклида; 3) расширенного алгоритма Евклида. Сравнить количество итераций. Написать программу, реализующую расширенный алгоритм Евклида.

Вариант 1. $a = 451, b = 3977$.

Вариант 2. $a = 3102, b = 4277$.

Вариант 3. $a = 901, b = 4717$.

Вариант 4. $a = 1463, b = 6391$.

Вариант 5. $a = 3289, b = 11297$.

Вариант 6. $a = 1711, b = 4189$.

Вариант 7. $a = 1891, b = 4087$.

Вариант 8. $a = 1739, b = 2867$.

Вариант 9. $a = 2911, b = 4189$.

Вариант 10. $a = 3713, b = 4187$.

Вариант 11. $a = 4399, b = 3403$.

Вариант 12. $a = 5251, b = 4183$.

Вариант 13. $a = 5551, b = 3367$.

Вариант 14. $a = 6499, b = 5335$.

Вариант 15. $a = 7171, b = 3131$.

Вариант 16. $a = 9559, b = 3509$.

Вариант 17. $a = 4067, b = 1127$.

Вариант 18. $a = 8099, b = 2275$.

Вариант 19. $a = 7553, b = 1411$.

Вариант 20. $a = 8633, b = 1157$.

Вариант 21. $a = 2291, b = 7663$.

Вариант 22. $a = 2201, b = 6461$.

Вариант 23. $a = 3367, b = 8099$.

Вариант 24. $a = 2120, b = 4399$.

Вариант 25. $a = 2679, b = 4503$.

Вариант 26. $a = 3233, b = 1769$.

Вариант 27. $a = 3953, b = 1541$.

Вариант 28. $a = 4740, b = 3871$.

Вариант 29. $a = 4970, b = 1917$.

Вариант 30. $a = 4970, b = 923$.

Лабораторная работа №2
«Сравнение первой степени»

Задание. Решить сравнение первой степени при помощи функции Эйлера. Написать программу, реализующую решение сравнения первой степени.

Вариант 1. $15x \equiv 21(mod\ 18)$.

Вариант 2. $12x \equiv 16(mod\ 28)$.

Вариант 3. $18x \equiv 12(mod\ 30)$.

Вариант 4. $7x \equiv 15(mod\ 25)$.

Вариант 5. $75x \equiv 54(mod\ 21)$.

Вариант 6. $37x \equiv 16(mod\ 11)$.

Вариант 7. $39x \equiv 5(mod\ 11)$.

Вариант 8. $20x \equiv 35(mod\ 45)$.

Вариант 9. $183x \equiv 93(mod\ 111)$.

Вариант 10. $19x \equiv 4(mod\ 25)$.

Вариант 11. $11x \equiv 15(mod\ 24)$.

Вариант 12. $39x \equiv 19(mod\ 53)$.

Вариант 13. $45x \equiv 21(mod\ 132)$.

Вариант 14. $12x \equiv 15(mod\ 35)$.

Вариант 15. $21x \equiv 10(mod\ 25)$.

Вариант 16. $15x \equiv 7(mod\ 16)$.

Вариант 17. $8x \equiv 17(mod\ 23)$.

Вариант 18. $64x \equiv 51(mod\ 13)$.

Вариант 19. $15x \equiv 21(mod\ 6)$.

Вариант 20. $57x \equiv 15(mod\ 48)$.

Вариант 21. $64x \equiv 5(mod\ 13)$.

Вариант 22. $139x \equiv 7(mod\ 8)$.

Вариант 23. $14x \equiv 9(mod\ 37)$.

Вариант 24. $32x \equiv 13(mod\ 15)$.

Вариант 25. $42x \equiv 105(mod\ 245)$.

Вариант 26. $29x \equiv 35(mod\ 123)$.

Вариант 27. $21x \equiv 15(mod\ 111)$.

Вариант 28. $15x \equiv 120(mod\ 85)$.

Вариант 29. $8x \equiv 15(mod\ 29)$.

Вариант 30. $8x \equiv 17(mod\ 31)$.

Лабораторная работа №3
«Символ Лежандра»

Задание. Найти символ Лежандра $\left(\frac{n}{p}\right)$. Написать программу, реализующую поиск символа Лежандра.

Для заданий лабораторной работы N – номер варианта, который указывается преподавателем. Значения n, p находятся по следующим правилам:

$$n = \begin{cases} 30N + 7, \text{если } N < 10 \\ 15N - 11, \text{если } N > 10 \end{cases}$$

$$p = \begin{cases} 937, \text{если } N \equiv 0(mod\ 5) \\ 941, \text{если } N \equiv 1(mod\ 5) \\ 947, \text{если } N \equiv 2(mod\ 5) \\ 953, \text{если } N \equiv 3(mod\ 5) \\ 967, \text{если } N \equiv 4(mod\ 5) \end{cases}$$

Лабораторная работа №4
«Квадратичное сравнение»

Задание. Решить квадратичное сравнение по простому модулю. Написать программу, реализующую решение квадратичных сравнений.

Вариант 1. а) $x^2 \equiv 34(mod\ 37)$ б) $x^2 \equiv 13(mod\ 23)$	Вариант 11. а) $x^2 \equiv 27(mod\ 37)$ б) $x^2 \equiv 18(mod\ 31)$	Вариант 21. а) $x^2 \equiv 14(mod\ 31)$ б) $x^2 \equiv 43(mod\ 53)$
Вариант 2. а) $x^2 \equiv 24(mod\ 53)$ б) $x^2 \equiv 19(mod\ 31)$	Вариант 12. а) $x^2 \equiv 33(mod\ 37)$ б) $x^2 \equiv 5(mod\ 19)$	Вариант 22. а) $x^2 \equiv 8(mod\ 73)$ б) $x^2 \equiv 10(mod\ 31)$
Вариант 3. а) $x^2 \equiv 10(mod\ 41)$ б) $x^2 \equiv 3(mod\ 23)$	Вариант 13. а) $x^2 \equiv 2(mod\ 31)$ б) $x^2 \equiv 28(mod\ 29)$	Вариант 23. а) $x^2 \equiv 22(mod\ 29)$ б) $x^2 \equiv 8(mod\ 31)$
Вариант 4. а) $x^2 \equiv 23(mod\ 29)$ б) $x^2 \equiv 6(mod\ 43)$	Вариант 14. а) $x^2 \equiv 50(mod\ 73)$ б) $x^2 \equiv 19(mod\ 31)$	Вариант 24. а) $x^2 \equiv 18(mod\ 73)$ б) $x^2 \equiv 13(mod\ 43)$
Вариант 5. а) $x^2 \equiv 18(mod\ 23)$ б) $x^2 \equiv 7(mod\ 29)$	Вариант 15. а) $x^2 \equiv 19(mod\ 101)$ б) $x^2 \equiv 7(mod\ 31)$	Вариант 25. а) $x^2 \equiv 6(mod\ 43)$ б) $x^2 \equiv 20(mod\ 29)$
Вариант 6. а) $x^2 \equiv 48(mod\ 73)$ б) $x^2 \equiv 12(mod\ 23)$	Вариант 16. а) $x^2 \equiv 54(mod\ 73)$ б) $x^2 \equiv 17(mod\ 59)$	Вариант 26. а) $x^2 \equiv 24(mod\ 73)$ б) $x^2 \equiv 21(mod\ 79)$
Вариант 7. а) $x^2 \equiv 2(mod\ 73)$ б) $x^2 \equiv 21(mod\ 43)$	Вариант 17. а) $x^2 \equiv 28(mod\ 31)$ б) $x^2 \equiv 60(mod\ 61)$	Вариант 27. а) $x^2 \equiv 21(mod\ 43)$ б) $x^2 \equiv 5(mod\ 29)$
Вариант 8. а) $x^2 \equiv 3(mod\ 61)$ б) $x^2 \equiv 8(mod\ 23)$	Вариант 18. а) $x^2 \equiv 5(mod\ 41)$ б) $x^2 \equiv 3(mod\ 83)$	Вариант 28. а) $x^2 \equiv 61(mod\ 73)$ б) $x^2 \equiv 21(mod\ 43)$
Вариант 9. а) $x^2 \equiv 32(mod\ 73)$ б) $x^2 \equiv 6(mod\ 23)$	Вариант 19. а) $x^2 \equiv 20(mod\ 31)$ б) $x^2 \equiv 26(mod\ 37)$	Вариант 29. а) $x^2 \equiv 15(mod\ 17)$ б) $x^2 \equiv 38(mod\ 43)$
Вариант 10. а) $x^2 \equiv 15(mod\ 53)$ б) $x^2 \equiv 5(mod\ 31)$	Вариант 20. а) $x^2 \equiv 40(mod\ 41)$ б) $x^2 \equiv 19(mod\ 67)$	Вариант 30. а) $x^2 \equiv 14(mod\ 43)$ б) $x^2 \equiv 47(mod\ 53)$

Лабораторная работа №5
«Система сравнений первой степени»

Задание. Решить систему сравнений первой степени. Написать программу, реализующую решение системы сравнений первой степени.

Вариант 1. $\begin{cases} x \equiv 10(mod\ 21) \\ x \equiv 6(mod\ 15) \\ x \equiv 19(mod\ 24) \end{cases}$	Вариант 2. $\begin{cases} x \equiv 7(mod\ 15) \\ x \equiv 23(mod\ 35) \\ x \equiv 13(mod\ 20) \end{cases}$
Вариант 3. $\begin{cases} 3x \equiv 5(mod\ 7) \\ 2x \equiv 3(mod\ 5) \\ 3x \equiv 3(mod\ 9) \end{cases}$	Вариант 4. $\begin{cases} x \equiv 2(mod\ 12) \\ x \equiv 12(mod\ 15) \\ x \equiv 3(mod\ 33) \end{cases}$
Вариант 5. $\begin{cases} x \equiv 32(mod\ 40) \\ x \equiv 23(mod\ 72) \\ x \equiv 13(mod\ 24) \end{cases}$	Вариант 6. $\begin{cases} x \equiv 6(mod\ 15) \\ x \equiv 18(mod\ 21) \\ x \equiv 3(mod\ 12) \end{cases}$
Вариант 7. $\begin{cases} x \equiv 13(mod\ 14) \\ x \equiv 6(mod\ 35) \\ x \equiv 26(mod\ 45) \end{cases}$	Вариант 8. $\begin{cases} x \equiv 19(mod\ 56) \\ x \equiv 3(mod\ 24) \\ x \equiv 7(mod\ 20) \end{cases}$
Вариант 9. $\begin{cases} x \equiv 19(mod\ 22) \\ x \equiv 8(mod\ 33) \\ x \equiv 14(mod\ 21) \end{cases}$	Вариант 10. $\begin{cases} 4x \equiv 9(mod\ 7) \\ 2x \equiv 15(mod\ 9) \\ 5x \equiv 12(mod\ 13) \end{cases}$
Вариант 11. $\begin{cases} 3x \equiv 2(mod\ 13) \\ 5x \equiv 11(mod\ 16) \\ 5x \equiv 2(mod\ 9) \end{cases}$	Вариант 12. $\begin{cases} 3x \equiv 5(mod\ 13) \\ 2x \equiv 17(mod\ 21) \\ 5x \equiv 31(mod\ 32) \end{cases}$
Вариант 13. $\begin{cases} x \equiv 1(mod\ 4) \\ x \equiv 3(mod\ 5) \\ x \equiv 2(mod\ 7) \end{cases}$	Вариант 14. $\begin{cases} x \equiv 2(mod\ 3) \\ x \equiv 2(mod\ 7) \\ x \equiv -2(mod\ 11) \end{cases}$

Вариант 15. $\begin{cases} 3x \equiv 5 (mod\ 14) \\ 5x \equiv 1 (mod\ 9) \\ 7x \equiv 2 (mod\ 25) \end{cases}$	Вариант 16. $\begin{cases} 7x \equiv 4 (mod\ 15) \\ 3x \equiv 23 (mod\ 28) \\ 5x \equiv 8 (mod\ 11) \end{cases}$
Вариант 17. $\begin{cases} 2x \equiv 5 (mod\ 21) \\ 5x \equiv 22 (mod\ 31) \\ 4x \equiv 5 (mod\ 29) \end{cases}$	Вариант 18. $\begin{cases} 3x \equiv 5 (mod\ 12) \\ 7x \equiv 3 (mod\ 25) \\ 3x \equiv 2 (mod\ 17) \end{cases}$
Вариант 19. $\begin{cases} x \equiv 8 (mod\ 15) \\ x \equiv 9 (mod\ 13) \\ x \equiv 5 (mod\ 14) \end{cases}$	Вариант 20. $\begin{cases} x \equiv 10 (mod\ 11) \\ x \equiv 9 (mod\ 16) \\ x \equiv 5 (mod\ 7) \end{cases}$
Вариант 21. $\begin{cases} x \equiv 5 (mod\ 3) \\ x \equiv 7 (mod\ 10) \\ x \equiv 2 (mod\ 7) \end{cases}$	Вариант 22. $\begin{cases} x \equiv 14 (mod\ 19) \\ x \equiv 5 (mod\ 7) \\ x \equiv 9 (mod\ 10) \end{cases}$
Вариант 23. $\begin{cases} x \equiv 8 (mod\ 13) \\ x \equiv 9 (mod\ 17) \\ x \equiv 5 (mod\ 11) \end{cases}$	Вариант 24. $\begin{cases} x \equiv 5 (mod\ 9) \\ x \equiv 3 (mod\ 5) \\ x \equiv 1 (mod\ 7) \end{cases}$
Вариант 25. $\begin{cases} x \equiv 12 (mod\ 13) \\ x \equiv 10 (mod\ 11) \\ x \equiv 5 (mod\ 12) \end{cases}$	Вариант 26. $\begin{cases} 5x \equiv 2 (mod\ 12) \\ 7x \equiv 2 (mod\ 8) \\ 3x \equiv 1 (mod\ 5) \end{cases}$
Вариант 27. $\begin{cases} 3x \equiv 8 (mod\ 20) \\ 5x \equiv 8 (mod\ 9) \\ 4x \equiv 1 (mod\ 21) \end{cases}$	Вариант 28. $\begin{cases} 2x \equiv 9 (mod\ 15) \\ 5x \equiv 4 (mod\ 7) \\ 7x \equiv 3 (mod\ 9) \end{cases}$
Вариант 29. $\begin{cases} 8x \equiv 1 (mod\ 13) \\ 5x \equiv 7 (mod\ 18) \\ 2x \equiv 1 (mod\ 9) \end{cases}$	Вариант 30. $\begin{cases} 3x \equiv 1 (mod\ 25) \\ 6x \equiv 3 (mod\ 33) \\ 4x \equiv 5 (mod\ 9) \end{cases}$

Лабораторная работа № 6
«Непрерывные дроби»

Задание.

а) Представить число в виде непрерывной дроби.

б) Найти рациональное число, которое обращается в данную непрерывную дробь (двумя способами).

в) Решить сравнение первой степени с помощью непрерывных дробей.

Написать программу, реализующую решение сравнения первой степени с помощью непрерывных дробей.

	а)	б)	в)
Вариант 1.	$\frac{105}{38}$	$[0; 1, 2, 3, 4, 5]$	$57x \equiv 15 (mod\ 48)$.
Вариант 2.	$\frac{245}{83}$	$[0; 2, 5, 14, 14]$	$64x \equiv 5 (mod\ 13)$.
Вариант 3.	$\frac{235}{69}$	$[0; 2, 5, 1, 1, 2, 16]$	$139x \equiv 7 (mod\ 8)$.
Вариант 4.	$\frac{46}{19}$	$[-1; 1, 2, 22, 1, 4, 2]$	$14x \equiv 9 (mod\ 37)$.
Вариант 5.	$\frac{375}{824}$	$[0; 1, 9, 1, 3, 23]$	$32x \equiv 13 (mod\ 15)$.
Вариант 6.	$\frac{990}{577}$	$[2; 1, 3, 4, 1, 2]$	$42x \equiv 105 (mod\ 245)$.
Вариант 7.	$\frac{875}{576}$	$[0; 3, 1, 2, 7]$	$29x \equiv 35 (mod\ 123)$.
Вариант 8.	$-\frac{55}{117}$	$[2; 1, 1, 6, 8]$	$21x \equiv 15 (mod\ 111)$.
Вариант 9.	$\frac{71}{41}$	$[-1; 1, 2, 5, 6]$	$15x \equiv 120 (mod\ 85)$.
Вариант 10.	$-\frac{187}{64}$	$[0; 1, 4, 3, 2]$	$8x \equiv 15 (mod\ 29)$.
Вариант 11.	$\frac{30}{37}$	$[-3; 2, 1, 3, 1, 4]$	$8x \equiv 17 (mod\ 31)$.
Вариант 12.	$\frac{127}{52}$	$[-2; 1, 3, 4, 5, 2]$	$15x \equiv 21 (mod\ 18)$.
Вариант 13.	$\frac{24}{35}$	$[0; 4, 3, 2, 1, 5, 6]$	$12x \equiv 16 (mod\ 28)$.
Вариант 14.	1,23	$[-1; 5, 4, 3, 3]$	$18x \equiv 12 (mod\ 30)$.
Вариант 15.	$-\frac{71}{41}$	$[-2; 1, 3, 1, 4, 2]$	$7x \equiv 15 (mod\ 25)$.
Вариант 16.	$\frac{157}{225}$	$[2; 1, 3, 4, 2]$	$75x \equiv 54 (mod\ 21)$.

Вариант 17.	$\frac{999}{2195}$	$[2; 1, 19, 1, 3]$	$37x \equiv 16 (mod\ 11)$.
Вариант 18.	0,459	$[3; 2, 2, 6, 2]$	$39x \equiv 5 (mod\ 11)$.
Вариант 19.	$-\frac{251}{764}$	$[2; 2, 2, 1, 2]$	$20x \equiv 35 (mod\ 45)$.
Вариант 20.	0,907	$[0; 2, 5, 14, 14]$	$183x \equiv 93 (mod\ 111)$.
Вариант 21.	$\frac{163}{59}$	$[1; 1, 2, 1, 1, 13, 6]$	$19x \equiv 4 (mod\ 25)$.
Вариант 22.	$\frac{22}{81}$	$[1; 1, 1, 12, 1, 1, 2, 4]$	$11x \equiv 15 (mod\ 24)$.
Вариант 23.	$\frac{269}{106}$	$[-1; 1, 1, 7, 1, 6]$	$39x \equiv 19 (mod\ 53)$.
Вариант 24.	$-\frac{31}{99}$	$[1; 1, 2, 1, 2, 1, 2]$	$45x \equiv 21 (mod\ 132)$.
Вариант 25.	$\frac{43}{53}$	$[-2; 1, 30, 2]$	$12x \equiv 15 (mod\ 35)$.
Вариант 26.	$-\frac{177}{67}$	$[0; 1, 4, 3, 2]$	$21x \equiv 10 (mod\ 25)$.
Вариант 27.	$-\frac{241}{195}$	$[2; 2, 3, 1, 5]$	$15x \equiv 7 (mod\ 16)$.
Вариант 28.	$\frac{352}{1513}$	$[0; 1, 2, 5, 2]$	$8x \equiv 17 (mod\ 23)$.
Вариант 29.	$-\frac{182}{225}$	$[1; 4, 2, 1, 7]$	$64x \equiv 51 (mod\ 13)$.
Вариант 30.	$-\frac{64}{53}$	$[-2; 3, 1, 2, 1, 2]$	$15x \equiv 21 (mod\ 6)$.