Задачи и упражнения.

Упражнения к Главе 1.

1. Вычислить НОД(a,b) при помощи алгоритма Евклида с делением с остатком и бинарного алгоритма Евклида. Сравнить количество итераций.

a) a = 715, b = 195; d) a = 1818, b = 726; g) a = 2448, b = 1632;

b) a = 246, b = 396; e) a= 6887, b = 6319; h) a = 1600, b = 1120;

c) a = 175, b = 14945; f) a = 1763, b = 1634; i) a = 2310, b = 3388.

j) a=210, b=34; k) a=27, b=307; l) a=264, b=320;

m) a=18, b=35; n) a=329, b=826; o) a=26, b=738;

p) a=288, b=15. q) a = 212, m =396; r) a = 212, m =144;

s) a = 212, m =156; t) a = 121, m =171; u) a = 112, m =184;

v) a = 122, m =196; w) a = 212, m =208; x) a = 122, m =250;

y) a = 112, m =240; z) a = 212, m =280;

2. Пользуясь таблицей простых чисел, найти канонические разложения следующих чисел:

a) 49200; d) 4144; g) 624239;

b) 22011; e) 2597; h) 422375;

c) 7533; f) 425106; i) 11502.

j) 21034; k) 27307; l) 264320;

m) 1835; n) 32926; o) 26738;

p) 28815. q) n=1345; r) n=1421;

s) n=1535; t) n=1721; u) n=1864;

v) n=1956; w) n=2078; x) n=2588;

y) n=2469; z) n=2822;

3. Вычислить НОК(a,b).

a) a = 744, b = 198; d) a = 50, b = 42; g) a = 3131, b = 808;

b) a = 60, b = 1575; e) a= 231, b = 1089; h) a = 1063, b = 3;

c) a = 128, b = 81; f) a = 73, b = 219; i) a = 1960, b = 1232.

j) a = 120, m =21; k) a = 112, m =27; l) a = 121, m =26;

m) a = 12, m =5; n) a = 122, m =8; o) a =2 12, m =10;

p) a = 112, m =12; q) a = 212, m =13; r) a = 212, m =14;

s) a = 212, m =15; t) a = 121, m =17; u) a = 112, m =18;

v) a = 122, m =19; w) a = 212, m =20; x) a = 122, m =25;

y) a = 112, m =24; z) a = 212, m =28;

4. Пользуясь свойствами функции Эйлера, вычислить φ(a).

a) a = 73; d) a = 343; g) a = 210;

b) a = 81; e) a= 6; h) a = 10800;

c) a = 97; f) a = 28; i) a = 32,

j) a = 2134; k) a = 2737; l) a = 432;

m) a = 343, n) a = 8! o)2424

p) a = 135; q) a = 170; r) a = 91;

s) a = 16; t) a = 64; u) a = 24;

v) a = 227; w) a = 725; x) a = 94836.

1.5. Выяснить, верны ли сравнения :

a) 25 ≡ —1 (mod 13); d) 3 ≡ 15 (mod 11); g) 128 ≡ 20 (mod 9);

b) 11 ≡ 3 (mod 2); e) 45 ≡ 12 (mod 11); h) 32 ≡ 5 (mod 7);

c) 100 ≡ 14 (mod 17); f) 98 ≡ 46 (mod 5); i) 13 ≡ 1 (mod 14).

j) 134≡5 (mod 19); k) 737≡7(mod 9); l) 432≡9 (mod 13);

m) 16≡3 (mod 13); n) -1≡1 (mod 5); o) -3≡5(mod 8);

p) 32≡0 (mod 4). q) 170≡-1(mod 19); r) 91≡-5(mod 12);

s) 161≡ -3 (mod 15); t) 64≡-2 (mod 3); u) 24≡-2(mod 2);

v) 227 ≡-3 (mod 5) w) 20≡ -16(mod12); x) 25≡-10(mod 7) ;

y) 24≡-9 (mod 5); z) 28≡-10 (mod 9);

1.6. Выписать полную и приведенную системы вычетов по модулю *n*. Сравнить количество чисел в приведенной системе вычетов со значением функции Эйлера от *n*.

a) *n* = 7; b) *n* = 9; c) *n* = 11; d) *n* = 16; e) *n* = 6; f) *n* = 2; g) n=23; h) n=22

i) n=3; j) n=21; k) n=27; l) n=26; m) n=5; n) n=8; o) n=10; p) n=12;

q) n=13; r) n=14; s) n=15; t) n=17; u) n=18; v) n=19; w) n=20; x) n=25;

y) n=24; z) n=28;

1.7. Вычислить абсолютно наименьший и наименьший неотрицательный вычеты числа *a* по модулю *m*.

a) *a* = 12, *m* = 15; d) *a* = 50, *m* = 12; g) *a* = —80 , *m* = 100;

b) *a* = 35, *m* = 31; e) *a*= 8, *m* = 15; h) *a* = —4, *m* = 3;

c) *a* = —1, *m* = 81; f) *a* = 8, *m* = 17; i) *a* = 11, *m* = 11.

j) *a* = 120, *m* =21; k) *a* = 112, *m* =27; l) *a* = 121, *m* =26;

m) *a* = 12, *m* =5; n) *a* = 122, *m* =8; o) *a* =2 12, *m* =10;

p) *a* = 112, *m* =12; q) *a* = 212, *m* =13; r) *a* = 212, *m* =14;

s) *a* = 212, *m* =15; t) *a* = 121, *m* =17; u) *a* = 112, *m* =18;

v) *a* = 122, *m* =19; w) *a* = 212, *m* =20; x) *a* = 122, *m* =25;

y) *a* = 112, *m* =24; z) *a* = 212, *m* =28;

1.8. Вычислить обратный элемент, если он существует:

a) 5^{-1} mod 8; d) 14^{-1} mod 25; g) 46^{-1} mod 51;

b) 7^{-1} mod 41; e) 13^{-1} mod 92; h) 77^{-1} mod 101;

c) 23^{-1} mod 63; f) 9^{-1} mod 27; i) 22^{-1} mod 25.

j) 25^{-1} mod 63; k) 7^{-1} mod 27; l) 21^{-1} mod 25.

m) 27^{-1} mod 63; n) 5^{-1} mod 27; o) 2^{-1} mod 25.

p) 29^{-1} mod 63; q) 3^{-1} mod 27; r) 23^{-1} mod 25.

s) 28^{-1} mod 63; t) 2^{-1} mod 27; u) 24^{-1} mod 25.

v) 26^{-1} mod 63; w) 4^{-1} mod 27; x) 3^{-1} mod 25.

y) 7^{-1} mod 8;   z) 3^{-1} mod 8;

1.9. Пользуясь теоремой Эйлера, вычислить:

a) 90^{42} mod 41; d) 8^{485} mod 187; g) 3^{161613} mod 16;

b) 34^{160003} mod 15; e) $(-2)^{634178}$ mod 117; h) 5^{186609} mod 9;

c) $(-5)^{100016}$ mod 11; f) 50^{190021} mod 38; i) 347^{174007} mod 349;

j) 25^{60} mod 61; k) 7^{153} mod 17; l) 21^{124} mod 25.

m) 27^{156} mod 63; n) 5^{134} mod 27; o) 2^{4524} mod 25.

p) 29^{1000} mod 63; q) 3^{234} mod 27; r) 23^{567} mod 25.

s) 28^{5674} mod 63; t) 2^{3456} mod 27; u) 24^{5678} mod 25.

v) 26^{7899} mod 63; w) 4^{2000} mod 27; x) 3^{1000} mod 25.

y) 7^{1000} mod 8;   z) 3^{100000} mod 8;

1.10. Решить сравнения:

a) $5x \equiv 3$(mod 11); d) $6x \equiv 15$(mod 21); g) $13x \equiv 8$(mod 16);

b) $8x \equiv 5$(mod 13); e) $16x \equiv 26$(mod 62); h) $25x \equiv 50$(mod 125);

c) $15x \equiv 25$(mod 17); f) $21x \equiv 14$(mod 42); i) $13x \equiv 37$(mod 29) j)7x≡3(mod 13);   k)-15x≡15(mod 35); l)35x≡5(mod 24);

m)18x≡13(mod 81). n) 3x≡1(mod 4)   o)2x≡3(mod 5)

p) 3x≡5(mod 7)   q) 2x≡1(mod 3)

r) 6x≡7(mod 11)   s) 3x≡1(mod 5)

t) 5x≡3(mod 7)   u) 7x≡2(mod 9)

v) 2x≡4(mod 5)   v) 3x≡5(mod 7)

w) 5x≡3(mod 8)

x) x≡2(mod 3)   y)6x≡5(mod 11)   z) 3x≡2(mod 4)

1.11. Решить системы сравнений.

a) $\begin{cases} x \equiv 3 \pmod{5} \\ x \equiv 8 \pmod{7} \end{cases}$; c) $\begin{cases} 2x \equiv 18 \pmod{22} \\ 3x \equiv 5 \pmod{7} \end{cases}$;e) $\begin{cases} 5x \equiv 3 \pmod{25} \\ x \equiv 8 \pmod{13} \end{cases}$;

b) $\begin{cases} x \equiv 1 \pmod{3} \\ x \equiv 2 \pmod{5} \\ x \equiv 3 \pmod{7} \end{cases}$; d) $\begin{cases} x \equiv 1 \pmod{4} \\ x \equiv 2 \pmod{9} \\ x \equiv 1 \pmod{5} \end{cases}$; f) $\begin{cases} 3x \equiv 18 \pmod{30} \\ x \equiv 2 \pmod{3} \\ 5x \equiv 1 \pmod{7} \end{cases}$.

g) 3x≡1(mod 4) 2x≡3(mod 5)

h) 3x≡5(mod 7) 2x≡1(mod 3)

i) 6x≡7(mod 11) 3x≡1(mod 5)

j) 5x≡3(mod 7) 7x≡2(mod 9)

k) 2x≡4(mod 5) 3x≡5(mod 7) 5x≡3(mod 8)

l) x≡2(mod 3) 6x≡5(mod 11) 3x≡2(mod 4)

m) x≡(2-1)(mod 7) 4x≡11(mod 13) 16x≡5(mod 19)

n) x≡3(mod 5) x≡1(mod 7) x≡4(mod 9)

o) x≡2(mod 5) x≡3(mod 11) x≡4(mod 17)

p) $x \equiv 1 \pmod 2$ $x \equiv 2 \pmod 3$ $x \equiv 4 \pmod 5$ $x \equiv 3 \pmod 7$

q) $x \equiv 2 \pmod 3$ $x \equiv 3 \pmod 4$ $x \equiv 6 \pmod 7$ $x \equiv 5 \pmod{11}$

1.12. Вычислить, пользуясь свойствами символа Якоби:

a) $\left(\frac{5}{7}\right)$; c) $\left(\frac{38}{11}\right)$; e) $\left(\frac{25}{30}\right)$; g) $\left(\frac{385}{927}\right)$; i) $\left(\frac{331}{221}\right)$; k) $\left(\frac{203}{313}\right)$;

b) $\left(\frac{2}{13}\right)$; d) $\left(\frac{150}{19}\right)$; f) $\left(\frac{343}{585}\right)$; h) $\left(\frac{54}{101}\right)$; j) $\left(\frac{222}{431}\right)$; l) $\left(\frac{928}{385}\right)$;

m) $\left(\frac{237}{359}\right)$ n) $\left(\frac{355}{469}\right)$ $o)$ $\left(\frac{142}{267}\right)$ p) $\left(\frac{218}{231}\right)$

q) (61/ 103) ; r) (73/109) ; s) (123/ 9);

t) (201 /49) ; u) (241 /148) ; w) (459 /175)

1.13. Решить следующие квадратичные сравнения по простому модулю, если решение существует.

a) $x^2 \equiv 17 \pmod{19}$; d) $x^2 \equiv 2 \pmod 7$; g) $x^2 \equiv 3 \pmod{41}$;

b) $x^2 \equiv 3 \pmod{13}$; e) $x^2 \equiv 3 \pmod{11}$; h) $x^2 \equiv 2 \pmod{17}$;

c) $x^2 \equiv 8 \pmod{41}$; f) $2x^2 \equiv 10 \pmod{11}$; i) $3x^2 \equiv 15 \pmod{31}$.

j) $x^2 \equiv 20 \pmod{31}$; k) $x^2 \equiv 13 \pmod{23}$; l) $x^2 \equiv 24 \pmod{53}$;

m) $x^2 \equiv 11 \pmod{19}$; n) $x^2 \equiv 10 \pmod{13}$; o) $x^2 \equiv 15 \pmod{17}$;

p) $x^2 \equiv 10 \pmod{41}$; q) $x^2 \equiv 7 \pmod{19}$; r) $x^2 \equiv 6 \pmod{23}$;

s) $x^2 \equiv 114 \pmod{31}$; t) $x^2 \equiv 7 \pmod{37}$; u) $x^2 \equiv 13 \pmod{53}$;

w) $x^2 \equiv 19 \pmod{61}$;

1.14. Решить следующие квадратичные сравнения по составному модулю, если решение существует.

a) x^2≡7(mod 9); g) x^2≡1 (mod 32); m) x^2≡11 (mod 35);

b) x^2≡—1(mod 25); h) x^2≡67 (mod 81); n) x^2≡5 (mod 12);

c) x^2≡32(mod 49); i) x^2≡59 (mod 125); o) x^2≡9 (mod 20);

d) x^2≡1(mod 4); j) x^2≡4(mod 6); p) x^2≡31 (mod 105);

e) x^2≡3(mod 8); k) x^2≡1(mod 15); q) x^2≡4 (mod 105);

f) x^2≡9(mod 16); l) x^2≡1(mod 24); r) x^2≡ 16 (mod 75).

s) x^2≡91 (mod 243); t) x^2≡145 (mod 256);

u) x^2≡21 (mod 49); v) x^2≡2 (mod 55);

w) x^2≡89(mod 160).

1.15. Определить, сколько решений имеют сравнения.

a) x^2≡—1(mod 59); d) x^2≡ 17(mod 32); g) x^2≡1(mod 150);

b) x^2≡ 3(mod 83); e) x^2≡ 25(mod 96); h) x^2≡4(mod 343);

c) x^2≡ 1(mod 8); f) x^2≡ 2(mod 315); i) x^2≡1(mod 2).

j) x2≡20 (mod 31); k) x2≡21 (mod 49); l) x2≡2 (mod 55);

m) x2≡89(mod 160); n) x 2≡13 (mod 23); o) x 2≡24 (mod 53);

p) x 2≡10 (mod 41); q) x2≡71 (mod 77); r) x2≡7 (mod 9);

s) x2≡40 (mod 81); t) x2≡100 (mod 231); v) x2≡1 (mod 110);

v) x 2≡81 (mod 176); w) x 2≡17 (mod 57)

1.16. Выписать все квадраты и все псевдоквадраты из приведенной системы вычетов по модулю *n*.

a) *n* = 15; b) *n* = 21; c) *n* = 33; d) *n* = 6; e) *n* = 14; f) *n* = 35.

1.17. Указать, какие их приведенных ниже чисел являются числами Блюма.

a) 7; b) 21; c) 47; d) 469; e) 35; f) 59.

1.18. Отыскать p_8 и p_9 – 8-е и 9-е простые числа, представимые в виде $4k+3$. Составить число Блюма $n=p_8p_9$. На основе BBS-генератора с ключом $s_0=121$ составить ключевую последовательность длиной 10 бит.

1.19. Существуют ли первообразные корни по модулю n, и если существуют, то сколько их?

a) n = 15; b) n = 71; c) n = 53; d) n = 202; e) n = 16; f) n = 25.

1.20. Найти первообразные корни по следующим модулям:

a) 3; c) 27; e) 26; g) 43; i) 169; k) 89;

b) 9; d) 13; f) 18; h) 86; j) 4; l) 41.

Упражнения к Главе 2.

2.1. Вычислить сумму и произведение многочленов $f(x)$ и $g(x)$ на $Z_2[x]$:

a) $f(x)=x^7+x^5+x+1$, $g(x)=x^4+x+1$; c) $f(x)=x^8+x^2$, $g(x)=x^3+x^2+1$;

b) $f(x)=x^4+x$, $g(x)=x^2+1$; d) $f(x)=x^5$; $g(x)=x^5+x$.

2.2. Вычислить остаток от деления $f(x)$ на $g(x)$ на $Z_2[x]$.

a) $f(x)=x^8+x^4+x+1$, $g(x)=x^3+x+1$; c) $f(x)=x^{10}+x^2+x+1$, $g(x)=x^2+x+1$;

b) $f(x)=x^4+x$, $g(x)=x^2+x+1$; d) $f(x)=x^5+x^4+1$; $g(x)=x^2+x$.

2.3. Вычислить НОД($g(x)$,$f(x)$) на $Z_2[x]$.

a) $f(x)=x^6+x^5+x^3+x^2+1$, $g(x)= x^5+x^4+x+1$;

b) $f(x)=x^6+x^4$, $g(x)=x^4+1$;

c) $f(x)=x^4+x^3+x^2+x$, $g(x)=x^5+x^3$;

d) $f(x)=x^9+x^8+x$; $g(x)=x^7+x^4+x^3+1$.

Упражнения к Главе 3:

3.1. Осуществить 2-факторизацию следующих чисел, используя метод Ферма и метод квадратичного решета с решетами по модулям 4, 5, 7. Сравнить количество итераций для этих двух методов.

a) 12317; c) 7081; e) 551; g) 1679; i) 6111; k) 1221;

b) 851; d) 18161; f) 481; h) 7313; j) 1197; l) 609.

3.2. Осуществить 2-факторизацию следующих чисел, используя ро-метод Полларда.

a) 1183; b) 1881; c) 2597; d) 1057; e) 5461; f) 299.

3.3. Осуществить факторизацию следующих чисел, используя p—1 –метод Полларда.

a) 133; b) 209; c) 161; d) 527; e) 1393; f) 3277.

3.4. Вычислить следующие дискретные логарифмы, пользуясь алгоритмом «шаг младенца – шаг великана».

a) $\log_3 14 \bmod \varphi(31)$; b) $\log_5 42 \bmod \varphi(47)$; c) $\log_3 30 \bmod \varphi(89)$.

3.5. При помощи алгоритма исчисления порядка вычислить следующие дискретные логарифмы.

a) $\log_3 57 \bmod \varphi(89)$; b) $\log_3 61 \bmod \varphi(79)$; c) $\log_3 279 \bmod \varphi(587)$.