dz 5

16

а)

т.к. $\text{НОД}(e, m) = 1$, то e и m взаимнопросты

запишем $ed \equiv 1(m)$, как :

$ed = km + 1$

$ed - km = 1$

т.к. e и m взаимно просты, то существует решение этого диафантова уравнения

найти его можно при помощи расширенного алгоритма Евклида

б)

$P' = C^d\ (n) = (P^e\ (n))^d\ (n) = P^{ed}\ (n)$

заметим, что $m = \varphi(n)$,

По теореме Эйлера:

$P^m \equiv 1\ (n)$

Но в тоже время:

$ed \equiv 1\ (m)$

Значит :

$P^{ed} \equiv P\ (n)$

$\implies P' = P$

17

если сумма делится на число, то сумма остатков слагаемых по модулю этого числа равна 0.

Посмотрим на остатки(по модулю 11):

$0^{10} = 0$

для всех остальных остальных чисел по теореме Ферма:

$n^{p-1} = 1$

Но слагаемых 6, а значит каждое из них должно делиться на 11, тогда и их произведение делится на 11^6

18

$19x + 22y = -21$

19 и 22 взаимно просты значит точно есть решения у

$19a + 22b = 1$

$19(a + b) + 3b = 1$

$1(a + b) + 3(b + 6a + 6b) = 1$

$\begin{cases} a + b = 1 \\ 6a + 7b = 0 \end{cases}$

частное решение:

$a = 7, b = -6$

возьмем:

$x = -21a + 22t, y = -21b + 19t$

$x = -142 + 22t, y = 126 + 19t$

19

$39x \equiv 104\ (221)$

т.к. $39x = 221k + 104$, то

$3x = 17k + 8$

значит

$3x \equiv 8\ (17)$

$3x + 17y = 8$

у этого диафантова уравнения 1 серия решений, т.к. 3 и 17 взаимно просты

20

12, 11 и 5 взаимно просты

найдем решение у :

$\begin{cases} a \equiv 1(12) \\ a \equiv 0(11) \\ a \equiv 0(5) \end{cases}$

$a = 55 * 7 = 385$

теперь:

$$\begin{cases} b \equiv 0(12) \\ b \equiv 1(11) \\ b \equiv 0(5) \end{cases}$$

$b = 60 * 9 = 540$

и:

$$\begin{cases} c \equiv 0(12) \\ c \equiv 0(11) \\ c \equiv 1(5) \end{cases}$$

$c = 132 * 3 = 396$

тогда частное решение:

$x_0=-14a+6b+19c\equiv -2a+6b-c= -2*385+6*540 -396 = 2074 $

серия решений:

$x = 2074 + 660t = 94 + 660t$

21

$\text{НОД}(3^{168} - 1, 3^{140} - 1)$

$3^{168} - 1 = k(3^{140} - 1) + r$

$k = 3^{28}$

$3^{168} - 1 = 3^{168} - 3^{28} + r$

$r = 3^{28} - 1$

$\text{НОД}(3^{168} - 1, 3^{140} - 1) = \text{НОД}(3^{28} - 1, 3^{140} - 1)$

по аналогии:

$3^{140} - 1 = k(3^{28} - 1) + r$

$k = 3^{112}$

$3^{140} - 1 = 3^{140} - 3^{112} + k'(3^{28} - 1) + r$

$3^{112} - 1 = k'(3^{28} - 1) + r$

$3^{112} - 1 = 3^{112} - 3^{84}k''(3^{28} - 1) + r$

$\dots$

$3^{28} - 1 = k''''(3^{28} - 1) + r$

$r = 0$

$\text{НОД}(3^{168} - 1, 3^{140} - 1) = \text{НОД}(3^{28} - 1, 3^{140} - 1) = \text{НОД}(3^{28} - 1, k''''(3^{28} - 1)) = 3^{28} - 1$

22

$46 = 2 * 23$

решим вначале по модулю 2:

пойдем с самого верха:

$3 = 1$

$3^3 = 3^1 = 3 = 1$

и так далее:

$3^{3^{\cdots}} = 1^{1^{\cdots}} = 1$

теперь решим по модулю 23:

пойдем с самого верха:

$3 = 3$

$3^3 = 27 = 4$

$3^{3^3} = 3^4 = 81 = 12$

$3^{3^{3^3}}=3^{12} = 243^2*3 = 13*^23 = 169*3= 8*3 =24 =1$

$3^{3^{3^{3^3}}} = 3^1 = 3$

обнаружен цикл длины 4, значит:

$3^{3^{\cdots}} = 3$

теперь:

$$\begin{cases} 3^{3^{\cdots}} \equiv 1 (2) \\ 3^{3^{\cdots}} \equiv 3 (23) \end{cases}$$

$3^{3^{\cdots}} = 3$