Домашнее задание на девятую неделю

Бельденова Камила, 675

11 апреля 2017 г.

1	2	3	4	5	6	7	Σ

Задача 1. Покажите, как вычислить a^{54} за 7 умножений. Можно ли еще быстрее?

1) $a \cdot a = a^2$
2) $a^2 \cdot a^2 = a^4$
3) $a^4 \cdot a^4 = a^8$
4) $a \cdot a^8 = a^9$
5) $a^9 \cdot a^9 = a^{18}$
6) $a^9 \cdot a^{18} = a^{27}$
7) $a^{27} \cdot a^{27} = a^{54}$

Нет, быстрее нельзя.
Первым шагом так и останется $a \cdot a = a^2$. Пусть дальше мы получим $a^3 = a \cdot a^2$. Посмотрим сможем ли мы за оставшиеся 4 шага получить a^{54}:
3) $a^3 \cdot a^3 = a^6$
4) $a^6 \cdot a^6 = a^{12}$
5) $a^{12} \cdot a^{12} = a^{24}$
6) $a^{24} \cdot a^{24} = a^{48}$

a^{54} не получили $\Rightarrow$ вторым шагом оставим операцию $a^2 \cdot a^2 = a^4$. Тогда после третьего шага можем получить $a^5 = a \cdot a^4$, $a^6 = a^2 \cdot a^4$ или $a^8 = a^4 \cdot a^4$. В случае с a^5 максимум, что мы можем получить: a^{40} — за оставшиеся 3 шага. Если же на третьем шаге мы получим a^6, то на шестом максимум — a^{48} $\Rightarrow$ третьим шагом оставим операцию $a^4 \cdot a^4 = a^8$. На четвертом шаге можем получить: a^9, a^{10}, a^{12} и a^{16}. Рассуждая аналогично предыдущим шагам, придем к выводу, что рациональнее всего оставить операцию $a^8 \cdot a^8 = a^{16}$, чтобы добиться результата за наименьшее количество шагов. Аналогично рассуждаем и на пятом шаге, оставляя в алгоритме операцию $a^{16} \cdot a^{16} = a^{32}$. Заметим, что имея a, a^2, a^4, a^8, a^{16} и a^{32}, одним умножением мы не сможем получить a^{54}. Т. е. несмотря на то, что на каждом шаге мы оставляли максимальный результат, мы не смогли получить a^{54} быстрее, чем за 7 шагов $\Rightarrow$ быстрее, чем за 7 умножений вычислить нельзя.

Задача 2. Делится ли $4^{1356} - 9^{4824}$ на 35? Делится ли $5^{30000} - 6^{123456}$ на 35?

(a) По свойству мультипликативности функции Эйлера:
$\varphi(35) = \varphi(5) \cdot \varphi(7) = (5-1) \cdot (7-1) = 24$
По теореме Эйлера:
$4^{\varphi(35)} = 4^{24} \equiv 1 \pmod{35}$
$4^{1356} = 4^{1344+12} = 4^{24 \cdot 56} \cdot 4^{12} \equiv 1^{56} \cdot 4^{12} = 256^3 \equiv 11^3 = 11 \cdot 121 \equiv 11 \cdot 16 = 176 \equiv 1 \pmod{35}$
$9^{4824} = 9^{24 \cdot 201} \equiv 1^{201} \equiv 1 \pmod{35}$
$4^{1356} - 9^{4824} \equiv 1 - 1 \pmod{35} = 0 \pmod{35} \Rightarrow$ да, делится.

(b) $\varphi(31) = \varphi(30)$, т. к. 31 — простое число.
По теореме Эйлера:
$5^{\varphi(31)} = 5^{30} \equiv 1 \pmod{31}$
$5^{30000} = 5^{30 \cdot 1000} \equiv 1^{1000} \equiv 1 \pmod{31}$
$6^{123456} = 6^{30 \cdot 4115 + 6} \equiv 1^{4115} \cdot 6^6 = 36^3 \equiv 5^3 = 125 \equiv 1 \pmod{31}$
$5^{30000} - 6^{123456} \equiv 1 - 1 \pmod{31} = 0 \pmod{31} \Rightarrow$ да, делится.

Задача 3. Пусть F_k — k-ое число Фибоначчи.Найдите результат работы Алгоритма Евклида на паре $(F; F_{k+1})$.
Найдите также число итераций алгоритма.
$F_0 = 0, F_1 = 1, F_k = F_{k-1} + F_{k-2}, k \geq 2, k \in \mathbb{Z}$
Euclid:
$gcd(F_k; F_{k+1}) = gcd(F_k; F_{k+1} - F_k) = gcd(F_{k-1}; F_k)$ — это первый шаг
Вторым шагом будет: $gcd(F_{k-1}; F_k) = gcd(F_{k-1}; F_k - F_{k-1}) = gcd(F_{k-2}; F_{k-1})$
Продолжая выполнять алгоритм k шагов, придем к выводу:
$gcd(F_k; F_{k+1}) = gcd(F_1; F_2) = 1 \Rightarrow$ числа $F_k; F_{k+1}$.

Задача 4. Найдите обратные $20 \pmod{79}$, $3 \pmod{62}$.

1. $20a \equiv 1 \pmod{79}$
Euclid:

20	79
20	19
1	19
1	0

Extended Euclid:
$1 = 20 - 19 = 20 - (79 - 3 \cdot 20) = 20 - 79 + 3 \cdot 20 = 4 \cdot \underline{20} - 1 \cdot \underline{79}$
$20 \cdot 4 \equiv 1 \pmod{79}$.
Ответ: 4 является обратным к 20 по модулю 79.

2. $3a \equiv 1 \pmod{62}$
Euclid:

3	62
3	2
1	2
1	0

Extended Euclid:
$1 = 3 - 2 = 3 - (62 - 3 \cdot 20) = 3 - 62 + 3 \cdot 20 = 21 \cdot \underline{3} - 1 \cdot \underline{62}$
$3 \cdot 21 \equiv 1 \pmod{62}$.
Ответ: 21 является обратным к 3 по модулю 62.

Задача 5. Найдите все решения уравнения $35x = 10 \pmod{50}$.
Euclid:

50	35
15	35

15 5
0 5
$gcd(50; 35) = 5$
Разделим уравнение на 5:
$7x = 2 \pmod{10}$
Подберем решение x_0:
$7 \cdot 6 = 2 \pmod{10} \Rightarrow x_0 = 6$
$x = x_0 + i \cdot \frac{n}{d} = 6 + 10i$
$i = 0, \ldots, d - 1 = 0, \ldots, 4$
Ответ: $x_1 = 6$, $x_2 = 16$, $x_3 = 26$, $x_4 = 36$, $x_5 = 46$.

Задача 6. Найдите наименьшее натуральное число, имеющее остатки $2, 3, 1$ от деления на $5, 13, 7$ соответственно.

$$\begin{cases} a = 2 \pmod{5} \\ a = 3 \pmod{13} \\ a = 1 \pmod{7} \end{cases}$$

$n_1 = 5 \quad m_1 = 91$
$n_2 = 13 \quad m_2 = 35$
$n_3 = 7 \quad m_3 = 65$

(a) $5x_5 + 91y_5 = 1$
Euclid:
5 91
5 1
0 1
Extended Euclid:
$1 = 1 \cdot \underline{91} - \underline{5} \cdot 18$

$\boxed{91y_5=91}$

(b) $13x_{13} + 35y_{13} = 1$
Euclid:
13 35
13 9
4 9
4 1
0 1
Extended Euclid:
$1 = 9-2\cdot4 = 35-2\cdot13-2\cdot(13-9) = 35-2\cdot13-2\cdot(13-(35-2\cdot13)) = 35-4\cdot13+2\cdot35-4\cdot13 = \underline{3}\cdot35-\underline{8}\cdot13$

$\boxed{35y_{13}=105}$

(c) $7x_7 + 65y_7 = 1$
Euclid:
7 65
7 2
1 2
1 0
Extended Euclid:
$1 = 7 - 2 \cdot 3 = 7 - 3 \cdot (65 - 7 \cdot 9) = 7 - 3 \cdot 65 + 7 \cdot 27 = 28 \cdot \underline{7} - 3 \cdot \underline{65}$

$\boxed{65y_{13}=\text{-}195}$

$a = 2 \cdot 91 + 3 \cdot 105 - 195 = 302$
Ответ: 302.

Задача 7. Докажите, что в поле $\mathbb{F}_p = \mathbb{Z}/(p)$ выполняется равенство $(a+b)^p = a^p + b^p$.
$(a+b)^p = a^p + b^p = a^p + C_p^1 a^{p-1} b^1 + \ldots + C_p^{p-1} a b^{p-1} + b^p$

Запишем формулу для биномиального коэффициента:

$$C_p^k = \frac{p!}{k!(p-k)!} = \frac{1 \cdot \ldots \cdot p}{k!(p-k)!}.$$

Из формулы видно, что числа вида C_p^k $(k \notin 0, p)$ кратны p, а, значит, сравнимы с 0 по модулю p, поэтому имеем:

$$(a+b)^p \overset{mod p}{=} a^p + b^p$$

ч. т. д.