Домашнее задание 7

Ткачев Андрей, группа 166

2 ноября 2016 г.

Задача 1

1

Если $c|a$ и $c \nmid b$, то $a = ck_0$, $b = ck_1 + r$. Тогда $a + b = c(k_0 + k_1) + r$. $\Rightarrow$ $c \nmid (a + b)$.

Утверждение (1) верно.

2

7 не делится на 8, и 1 не делится на 8, но $1 + 7$ кратно 8.

Утверждение (2) неверно.

3

14 не делится на 8, и 12 не делится на 8, но $8 \mid 12 \cdot 14$.

Утверждение (3) не верно.

4

Если $c \mid a$ и $c \mid b$, то $a = ck_0$, $b = ck_1$. Тогда $ab = c^2 k_0 k_1$.

Значит $c^2 \mid ab$. Утверждение (4) верно.

Задача 2

А

Поймем, что $2^{15}|20!$, и более того: $2^{18}|20!$ Выпишем все четные множители, входящие в 20!:

$$2, 4, 6, 8, 10, 12, 14, 16, 18, 20$$

Посчитаем степень суммарную степень двойки, входящую в произведение:

$$1+2+1+3+1+2+1+4+1+2=18$$

Т.е. $20! = 2^{18} \cdot k \Rightarrow 20! \equiv 0 \mod 2^{15}$.

Б

Как мы еще помним, $2^{18}|20!$, а значит $20! = 2^{18} \cdot k$, причем $k = 2m+1$, т.е. 2 входит в 20! в степени 18. Значит $20! = 2^{18}(2m+1) = 2^{19}m + 2^{18}$.

Тогда $20! \equiv 2^{18} \mod 2^{19}$.

Задача 3

$x^2 \equiv 1(\mod 2^n) \Leftrightarrow x^2 - 1 \equiv 0(\mod 2^n)$

Тогда $(x-1)(x+1) \equiv 0 \mod 2^n$. Заменим $x - 1 = y$. Перепишем равенство:

$$y(y+2) \equiv 0 \mod 2^n \mathbf{(1)}$$

Нас интересуют те y, для которых верно $0 \leqslant y+1 < 2^n$ **(2)**.

$y = 0$, $y = 2^n - 2$ - решениями очевидно являются. Иначе: **(1)** $\Rightarrow y = a2^k$, $y + 2 = b2^m$, причем $2^n \leqslant m + k$ ($2 \nmid a, b$ и $a, b > 0$). Но тогда

$$y+2 = a2^k + 2 = 2(a2^{k-1}+1) = b2^m$$

$$a2^{k-1}+1 = b2^{m-1}$$

Значит либо $k = 1$, либо $m = 1$. В первом случае:

$$y+2 = a \cdot 2^{n-1}$$

$$y = a \cdot 2^{n-1} - 2.$$

Во втором:

$$y = b \cdot 2^{n-1}.$$

Поймем, что в силу **(2)** и того, что a и b не четны: a, $b = 1$.

Тогда получаем 4 решения y. Перейдем от них к x.

Ответ:

$$1$$

$$2^{n-1} \pm 1$$

$$2^n - 1$$

При $n = 2$ две пары решений эквивалентны.

Задача 4

Воспользуемся свойством, на котором основан алгоритм Евклида $(a, b) = (a - b, b)$, $a > b$.

$(2^{2016} - 1, 2^{450} - 1) = (2^{2016} - 2^{450}, 2^{450} - 1) = (2^{450}(2^{1556} - 1), 2^{450} - 1)$

Докажем, что если $(a, b) = 1$, а $(ak, b) = g$, то $(k, b) = g$.

$(a, b) = 1 \Rightarrow \exists x,\ y : ax + by = 1$ (Основная лемма арифметики остатков). Тогда $kax + kby = k$, так как $g|ak$ и $g|b$, то $g|k$. Заметим, что (k, b) не больше g (иначе $(ak, b) > g$), а значит в точности g. ◀

Т.к. $(2^{450}, 2^{450} - 1) = 1$, то

$$(2^{450}(2^{1556} - 1), 2^{450} - 1) = (2^{1556} - 1, 2^{450} - 1)$$

$$(2^{450}(2^{1116} - 1), 2^{450} - 1) = (2^{1116} - 1, 2^{450} - 1)$$

$$(2^{450}(2^{666} - 1), 2^{450} - 1) = (2^{666} - 1, 2^{450} - 1)$$

$$(2^{450}(2^{216} - 1), 2^{450} - 1) = (2^{216} - 1, 2^{450} - 1)$$

$$(2^{216}(2^{234} - 1), 2^{216} - 1) = (2^{216} - 1, 2^{234} - 1)$$

$$(2^{216}(2^{18} - 1), 2^{216} - 1) = (2^{216} - 1, 2^{18} - 1)$$

Поймем, что $2^{216} - 1 = (2^{108} - 1)(2^{108} + 1) = (2^{54} - 1)(2^{54} + 1)(2^{108} + 1) = (2^{27} - 1)(2^{27} + 1) \cdot ...$

Но

$$2^{27} - 1 = (2^9 - 1)(2^{18} + 2^9 + 1),$$
$$2^{27} + 1 = (2^9 + 1)(2^{18} - 2^9 + 1).$$

Тогда $2^{216} - 1 = (2^9 - 1)(2^9 + 1) \cdot ... = (2^{18} - 1) \cdot ...$

$$(2^{216} - 1, 2^{18} - 1) = 2^{18} - 1.$$

Ответ: $2^{18} - 1$.

Задача 5

$74x \equiv 1 \mod 47$

Поймем, что такой x существует, т.к. $(74, 47) = 1$. Найдем x решив уравнение $74x - 47y = 1$, пользуясь расширенным алгоритмом Евклида:

$$a_0 = 74 \cdot 1 - 47 \cdot 0$$

$$a_1 = 74 \cdot 0 + 47 \cdot 1$$

$$a_{i-2} = 74x_{i-2} + 47y_{i-2}$$

$$a_{i-1} = 74x_{i-1} + 47y_{i-1}$$

$$a_i = a_{i-2} \% a_{i-1} = a_{i-2} - a_{i-1} \lfloor \frac{a_{i-2}}{a_{i-1}} \rfloor = 74(x_{i-2-\lfloor \frac{a_{i-2}}{a_{i-1}} \rfloor} x_{i-1}) + 47(y_{i-2-\lfloor \frac{a_{i-2}}{a_{i-1}} \rfloor} y_{i-1})$$

$$a_2 = 74 \cdot 1 - 47 \cdot 1 = 27$$

$$a_3 = -74 \cdot 1 + 47 \cdot 2 = 20$$

$$a_4 = 74 \cdot 2 - 47 \cdot 3 = 7$$

$$a_5 = -74 \cdot 5 + 47 \cdot 8 = 6$$

$$a_6 = 74 \cdot 7 - 47 \cdot 11 = 1$$

Таким образом искомый вычет 7.
Ответ: 7.

Задача 6

Количество решений сравнения $39x \equiv 104 \mod 221$ равно количеству решений сравнения $3x \equiv 8 \mod 17$ умноженному на 13 (т.к. каждое решение нового сравнения меньше 17, но при этом, если к нему прибавить $17k$, то получим решение начального сравнения, $0 < k < 13$), т.к. $(39, 104, 221) = 13$.

$$3x \equiv 8 \mod 17$$

Т.к. 3 взаимно просто с 17, то можно обратить 3 по модулю.

$$3^{-1} \equiv 6 \mod 17$$

Домножим исходное на 6, получаем:

$$x \equiv 14 \mod 17$$

Это эквивалентно 13 решениям по модулю $17 \cdot 13$:

$$13, 13 + 17, 13 + 17 \cdot 2, ..., 13 + 17 \cdot 12.$$

Ответ: 13 решений.

Задача 7

Число делится на 22, если оно делится на 2 и на 11. Тогда $22|n^{10}-1$, если n нечетно и $11|n^{10}-1$. Очевидно, что n не должно делится на 11. Т.к. 11 - простое число, то по м. теореме Ферма: $n^{10} \equiv n \mod 11 \Rightarrow n \equiv 1 \mod 11$.

Ответ: для всех нечетных n, не делящихся на 11

Задача 8

Посмотрим внимательно на сумму:

$$1 + \frac{1}{2} + ... + \frac{1}{p-2} + \frac{1}{p-1}$$

Поймем про нее две вещи:

- Количество слагаемых четно
- Сумма слагаемых i и $p-i$ имеет вид: $\frac{p}{(p-i)i}$

Тогда разобьем сумму на такие парные слагаемые, раз всего слагаемых четное число. Получим сумму дробей, знаменатель которых p. Вынесем p, как общий множитель и сложим дроби $\frac{1}{1(p-1)} + \frac{1}{2(p-2)} + ...$, выполнив сокращение до несократимой, и умножим числитель на оставшуюся вне скобок p. Поймем, что мы получили несократимую дробь (p не делится ни одно из чисел $1..p-1$), которая равна начальной, а числитель ее кратен p, что мы и хотели доказать.