Домашнее задание по дискретной математике 2а

№1

Пусть $99^{1000} \equiv x \pmod{100}$. Тогда при нахождении x мы получим ответ.

$99^0 \equiv_{100} 1$

$99^1 \equiv_{100} 99$

$99^2 = 9801 \equiv_{100} 1$ ← получили цикл.

Легко видно, что $99^{1000} \equiv 1 \pmod{100}$ (чётный показатель степени)

Ответ: 0 1

№2

$$\underset{(*)}{\left(a^3 - b^3 \equiv 0 \pmod{(a-b)}\right)} \Rightarrow a^3 \equiv b^3 \pmod{(a-b)}$$

Докажем $(*)$:

$$(*) \Leftrightarrow (a-b)(a^2 + ab + b^2) \equiv 0 \pmod{(a-b)}$$

очевидно верно (множитель $(a-b)$ в левой части)

ч.т.д..

№3

Пусть $5m+3n=11k;\ k\in\mathbb{Z}$

$$\Downarrow$$

$$n=\frac{11k-5m}{3}$$

Тогда: $9m+n=\dfrac{27m+11k-5m}{3}=$

$=\dfrac{22m+11k}{3}=11\cdot\dfrac{2m+k}{3}$ - очевидно,

что это число делится на 11. Ч.т.д..

№4

а) Пусть $41^{24}\equiv x\ (\mathrm{mod}\ 97)$

Рассмотрим разл. остатки:

$41^0\equiv_{97}1$

$41^1\equiv_{97}41$

$41^2=41\cdot41=1681\equiv_{97}32$

$41^4=41^2\cdot41^2\equiv_{97}32\cdot32=1024\equiv_{97}54$

$41^8=41^4\cdot41^4\equiv_{97}54\cdot54=2916\equiv_{97}6$

$41^{16}=41^8\cdot41^8\equiv_{97}6\cdot6=36\equiv_{97}36$

$41^{24}=41^{16}\cdot41^8\equiv_{97}36\cdot6=216\equiv_{97}22$

Итого: $41^{24}\equiv22\ (\mathrm{mod}\ 97)$

б) Пусть $(-117)^{31}\equiv x\ (\mathrm{mod}\ 83)$

$-117=83\cdot(-2)+49\Rightarrow-117\equiv49\ (\mathrm{mod}\ 83)$

Тогда: $49^{31}\equiv x\ (\mathrm{mod}\ 83)$

Рассмотрим различные остатки:

$49^0\equiv_{83}1$

$49^1\equiv_{83}49$

$$49^2 = 49 \cdot 49 = 2401 \equiv_{83} 77$$

$$49^3 = 49^1 \cdot 49^2 \equiv_{83} 49 \cdot 77 = 3773 \equiv_{83} 38$$

$$49^5 = 49^2 \cdot 49^3 \equiv_{83} 77 \cdot 38 = 2926 \equiv_{83} 21$$

$$49^{10} = 49^5 \cdot 49^5 \equiv_{83} 21 \cdot 21 = 441 \equiv_{83} 26$$

$$49^{20} = 49^{10} \cdot 49^{10} \equiv_{83} 26 \cdot 26 = 676 \equiv_{83} 12$$

$$49^{30} = 49^{20} \cdot 49^{10} \equiv_{83} 12 \cdot 26 = 312 \equiv_{83} 63$$

$$49^{31} = 49^{30} \cdot 49^1 \equiv_{83} 63 \cdot 49 = 3087 \equiv_{83} 16$$

$$(-117)^{31} \equiv 16 \pmod{83}$$

№5

Пусть остаток $(x+M, 2M) =$
$= ost(x+M, 2M)$

При применении для x $I(x) =$
$= ost(x+M, 2M) - M$ мы берём остаток при делении $(x+M)$ на $2M$, получая число в диапазоне $[0; 2M-1]$, вычитая из него M мы возвращаемся в диапазон $[-M; M-1]$.

а) $x \in [-M; M-1] \Rightarrow x+M \in [0; 2M-1]$

Тогда $ost(x+M, 2M) = x+M$

$I(x) = x+M-M = x$; ч.т.д..

б) $I(x) = ost\,(x+M,\ 2M) - M$

Рассмотрим: $I(I(x) + I(y)) =$

$= ost\,(I(x) + I(y) + M,\ 2M) - M \quad (*)$

$I(x) + I(y) + M = ost\,(x+M,\ 2M) +$

$+ ost\,(y+M,\ 2M) - M \equiv$

$\equiv x + y + M \pmod{2M}$ (арифметика остатков)

Но в $(*)$, в первом слагаемом суммы, как раз и происходит сложение по модулю $2M$; тогда $(*)$ примет вид:

$ost\,(x+y+M,\ 2M) - M = I(x+y)$; ч.т.д..

в) $I(I(x) \cdot I(y)) = ost\,(I(x) \cdot I(y) + M,\ 2M) - M \quad (*)$

$I(x) = ost\,(x+M,\ 2M) - M \equiv$

$\equiv x + M - M \pmod{2M} \equiv x \pmod{2M}$

Тогда $(*)$ примет вид:

$ost\,(x \cdot y + M,\ 2M) - M = I(x\,y)$

ч.т.д..

№ 7

В задаче воспользуемся основной теоремой арифметики: $n = \prod_{i=1}^{k} p_i^{\alpha_i}$,

где $n \in \mathbb{N}$, p – простые числа.

Пусть x / n, тогда в разложении x не может быть простых сомножителей, отличных от тех, что присутствуют в разложении n.

$$x = \prod_{i=1}^{k} p_i^{\beta_i} \quad ; \quad 0 \leq \beta_i \leq \alpha_i$$

Тогда каждый α_i даёт $\alpha_i + 1$ новых делителей n. $\Rightarrow$ формула для общего кол-ва делителей $x \in \mathbb{N}$ имеет вид: $\prod_{i=1}^{k} (\alpha_i + 1)$

В нашем случае обозначим число h. Тогда т.к. $(2 / h) \wedge \neg (4 / h) \Rightarrow$ в разложении на простые у h 2 встречается ровно 1 раз.

$$h = 2^1 \cdot \prod_{i=2}^{k} p_i^{\alpha_i}$$

Найдём общее кол-во делителей h (обозн. как H_1):

$$H_1 = 1 + 1 \cdot \prod_{i=2}^{k} (\alpha_i + 1) = 2 \cdot \prod_{i=2}^{k} (\alpha_i + 1)$$

Заметим, что если не использовать 2 при составлении делителей, то сам делитель получится нечётный, т.к. $\forall$ простое число $\neq 2$ – нечётное.
Значит общее кол-во нечётных делителей (обозн. как H_2) можно найти по формуле:

$$H_2 = \prod_{i=2}^{r} (\alpha_i + 1)$$

Кол-во чётных делителей (обозн. как H_3):

$$H_3 = H_1 - H_2 = 2 \cdot \prod_{i=2}^{r} (\alpha_i + 1) - \prod_{i=2}^{r} (\alpha_i + 1) =$$

$$= \prod_{i=2}^{r} (\alpha_i + 1) = H_2$$; ч.т.д..

№8

Заметим, что сумма цифр этого числа равна $100 \cdot 0 + 100 \cdot 1 + 100 \cdot 2 = 300$
$\Rightarrow 3 \mid$ число, но $\neg(9 \mid \text{число})$, далее наше число обозначим через x.
Предположим, что x – полный квадрат, т.е.:
$x = h \cdot h$, где h – некоторое натуральное число
Предположим, что $\neg(3 \mid h)$ рассмотрим все возможные остатки $h \cdot h$ по модулю 3:
1) $h = 1$: $h \cdot h \equiv 1 \pmod 3$, но $3 \mid x \Rightarrow$
$\Rightarrow$ не подходит

2) $n = 2$: $n \cdot n \equiv 1 \pmod 3$, но $3 | x$ $\Rightarrow$

$\Rightarrow$ не подходит

Оба случая не подошли $\Rightarrow$ $3 | n$.

Но тогда в разложении n на простые 3 встречается хотя бы 1 раз $\Rightarrow$ в разложении $n \cdot n$ на простые 3 встречается хотя бы 2 раза $\Rightarrow$ $9 | n \cdot n$. Но $\neg(9 | x)$ — противоречие. Значит наше предположение неверно и x — не точный квадрат.

N 11

Любое целое число можно представить как $6k$, $6k+1$, $6k+2$, $6k+3$, $6k+4$, $6k+5$.

• $6k$ и $6k+3$ делятся на 3

• $6k+2$ и $6k+4$ делятся на 2

$\Rightarrow$ $\forall$ простое число представимо в виде $6k+1$ или $6k+5$ (больше 3)

Пусть простых чисел вида $6k+5$ конечное число: $\{p_1, p_2 \dots p_n\}$

Рассмотрим число:

$$K = 6 \cdot p_1 \cdot p_2 \cdot \ldots p_n - 1$$

• $K \equiv -1 \equiv 5 \pmod 6 \Rightarrow K = 6k+5$

• Ни одна из чисел $\{p_1, p_2 \dots p_n\}$ не делит K.

В разложении K есть хотя бы один простой делитель. Причём это не 2 и не 3, т.к. $K \equiv 5 \pmod 6$

$\Rightarrow$ этот простой делитель имеет вид $6k+1$ или $6k+5$.

Если все простые делители имеют вид $6k+1$, то: K - имеет вид $(6k+1)$, т.к.:

$(6k+1)\cdot(6k+1) = 36k^2+6k+6k+1 =$
$= 6k(6k+2)+1 \leftarrow$ число вида $6k+1$.

Но тогда все простые делители имеют вид $6k+5$ при. Но тогда это новое простое число вида $6k+5$, т.к. ни одно число

из $\{p_1, p_2 \ldots p_n\}$ не делит K.
Получили противоречие $\Rightarrow$ их бесконечное кол-во.