Решения задач по теме «Теория чисел»

1. Найдите все простые числа $p \geq 3$ и целые числа x, y, удовлетворяющие уравнению $x^{p-1} + x^{p-2} + ... + x + 2 = y^2$.

►Если $p = 3$, то $x^2 + x + 2 = y^2$. Отсюда $(2x+1)^2 + 7 = (2y)^2$, то есть $7 = (2y - 2x - 1)(2y + 2x + 1)$. Отсюда находим следующие варианты пар (x, y): $(1,2)$, $(1,-2)$, $(-2,2)$, $(-2,-2)$. Пусть $p > 3$. Рассмотрим произвольный простой делитель q числа $y^2 - 1$. Тогда $x^{p-1} + x^{p-2} + ... + x + 1 = y^2 - 1 \equiv 0 (\mathrm{mod}\, q)$. Следовательно, $x^p \equiv 1 (\mathrm{mod}\, q)$. Обозначим через r показатель, которому принадлежит число x по модулю q. Тогда $r \mid p$. Поэтому $r = p$ или $r = 1$. Если $r = 1$, то $x \equiv 1 (\mathrm{mod}\, q)$ и тогда $p \equiv 0 (\mathrm{mod}\, q)$, то есть $q = p$. Если $r = p$, то отсюда и из сравнения $x^{q-1} \equiv 1 (\mathrm{mod}\, q)$ вытекает, что $p \mid q - 1$, то есть $q \equiv 1 (\mathrm{mod}\, p)$. Таким образом, $y^2 - 1 = p^{\alpha}(t_1 p + 1)...(t_k p + 1)$, где $t_1, .., t_k \in Z$, $\alpha \in N \cup \{0\}$. Поэтому $y - 1 = p^{\beta}(t_1 p + 1)...(t_m p + 1), \quad y + 1 = p^{\gamma}(t_{m+1} p + 1)...(t_k p + 1)$. Отсюда следует, что числа $y - 1$, $y + 1$ сравнимы либо с 0, либо с 1 по модулю p, что невозможно при $p > 3$. ◄

2. Докажите, что для простых $p > 5$ и натуральных m равенство $(p-1)! + 1 = p^m$ невозможно.

►Допустим, существуют такие p, m. Тогда $p^m - 1 = (p-1)! \quad \Leftrightarrow \quad p^{m-1} + ... + p + 1 = (p-2)!$.

Так как $2 < \frac{p-1}{2} < p - 2$, то $p - 1 \mid (p-2)!$. Поскольку $p^i \equiv 1 (\mathrm{mod}\, p - 1)$, то $p^{m-1} + ... + p + 1 \equiv m (\mathrm{mod}\, p - 1)$. Следовательно, $p - 1 \mid m$. Поэтому $m \geq p - 1$. Отсюда получаем, что $(p-1)! + 1 \geq p^{p-1}$. Очевидно, это неравенство невозможно при $p > 5$.◄

3. Пусть натуральные числа a и b таковы, что $a^n + n \mid b^n + n$ для любого натурального n. Докажите, что $a = b$.

► Очевидно, что $b \geq a$. Предположим, что $b > a$. Возьмём произвольное простое число p, большее числа b. В силу китайской теоремы об остатках существует натуральное n, такое, что $n \equiv -a (\mathrm{mod}\, p)$, $n \equiv 1 (\mathrm{mod}\, p - 1)$. Так как $(a, p) = 1$, то $a^n = a^{t(p-1)+1} \equiv a (\mathrm{mod}\, p)$. Аналогично $b^n \equiv b (\mathrm{mod}\, p)$. Так как $n \equiv -a (\mathrm{mod}\, p)$, то $p \mid a^n + n$. Следовательно, $p \mid b^n + n$. Таким образом, $b^n + n \equiv b - a \equiv 0 (\mathrm{mod}\, p)$, что невозможно. Поэтому $a = b$.◄

4. Пусть n - натуральное число, α - комплексное число, такие, что числа α^n и $(\alpha+1)^n$ рациональные. Можно ли утверждать, что число α также рациональное?

►Нельзя, т.к. $i^4 = 1, (i+1)^4 = -4.$◄

5. Найдите все простые числа p и натуральные числа x, y, n, удовлетворяющие уравнению $x(x+1) = p^{2n} y(y+1)$.

► Так как $p^{2n} \mid x(x+1)$, то $p^{2n} \mid x$ либо $p^{2n} \mid x+1$. Следовательно, $x+1 \geq p^{2n}$.

$x(x+1) = p^{2n} y(y+1) \quad \Leftrightarrow \quad \left(p^n(2y+1)+(2x+1)\right)\left(p^n(2y+1)-(2x+1)\right) = p^{2n}-1$.

Так как $p^n(2y+1)+(2x+1) \mid p^{2n}-1$, то $p^{2n}-1 > 2x+1$. Тем самым получаем, что $p^{2n} > 2p^{2n}$. Решений нет. ◄

6. Найдите все натуральные x, удовлетворяющие равенству
$\varphi(2x) = \varphi(3x)$.

►Пусть $x = 2^a \cdot 3^b \cdot y$, где $(y,2) = (y,3) = 1$, тогда $\varphi(2x) = \varphi(2^{a+1} \cdot 3^b) \cdot \varphi(y)$, $\varphi(3x) = \varphi(2^a \cdot 3^{b+1}) \cdot \varphi(y)$. Поэтому $\varphi(2^{a+1} \cdot 3^b) = \varphi(2^a \cdot 3^{b+1})$. Случай $b > 0$ невозможен, так как тогда $\varphi(2^{a+1}) \cdot 3^{b-1} \cdot 2 = \varphi(2^a) \cdot 3^b \cdot 2$ (правая часть делится на 3^b, а левая нет). Следовательно, $\varphi(2^{a+1}) = \varphi(2^a \cdot 3) \Leftrightarrow \varphi(2^{a+1}) = 2\varphi(2^a)$. Последнее верно для любых натуральных a. Таким образом, x - любое чётное натуральное число, не делящееся на 3. ◄

7. Найдите все нечетные натуральные n, такие, что $n \mid 3^n + 1$.
► $n = 1$ подходит. Допустим, что $n > 1$. Пусть p - наименьший простой делитель числа n. Очевидно, $p > 3$. Обозначим через δ показатель, которому принадлежит число 3 по модулю p. Тогда имеем $p \mid 3^{p-1} - 1$, $p \mid 3^{2n} - 1$. Следовательно, $\delta \mid p-1$ и $\delta \mid 2n$. Допустим, что δ - нечетное число, тогда $\delta \mid n$. Так как $\delta < p$, то $\delta = 1$, что невозможно. Следовательно, δ - чётное число, то есть $\delta = 2k$. Тогда $k \mid n$, поэтому k - нечётное число. Если предположить, что $k > 1$, то, поскольку $k < p$ и $k \mid n$, найдётся простой делитель числа n, меньший p. Следовательно, $k = 1$, тогда $\delta = 2$, откуда получаем, что $p = 2$, а это невозможно. ◄

8. Пусть натуральное число a принадлежит показателю δ по модулю m. Для любого натурального числа γ найдите натуральное число, которое принадлежит показателю (δ, γ) по модулю m.

► Найдём натуральное число n, такое, что число a^n принадлежит показателю (δ,γ) по модулю m. Имеем: $(\delta,\gamma)=\dfrac{\delta}{(n,\delta)}$. Пусть $d=(\gamma,\delta)$, $\gamma=d\gamma_1$, $\delta=d\delta_1$, тогда $(\delta,\gamma)=\dfrac{\delta}{(n,\delta)} \Leftrightarrow (n,d\delta_1)=\delta_1$. Поэтому достаточно выбрать $n=\delta_1=\dfrac{\delta}{(\delta,\gamma)}$. ◄

9. Докажите, что многочлен $f(x)=x^7-14$ является неприводимым над Q.

►Достаточно применить признак Эйзенштейна при $p=2$.◄

10. Найдите минимальный многочлен для элемента $a=\sqrt[3]{1-\sqrt{2}}$.

► Так как $a^3=1-\sqrt{2}$, $(1-a^3)^2=2$, то минимальный многочлен $f(x)$ числа a делит многочлен $g(x)=x^6-2x^3-1$. Докажем, что $f(x)=g(x)$. Предположим противное. Многочлен $g(x)$ имеет два иррациональных действительных корня $\alpha_1=\sqrt[3]{1+\sqrt{2}}$, $\alpha_2=\sqrt[3]{1-\sqrt{2}}$ и четыре мнимых корня $\beta_1=\alpha_1\left(-\frac{1}{2}+i\frac{\sqrt{3}}{2}\right)$, $\beta_2=\alpha_1\left(-\frac{1}{2}-i\frac{\sqrt{3}}{2}\right)$, $\beta_3=\alpha_2\left(-\frac{1}{2}+i\frac{\sqrt{3}}{2}\right)$, $\beta_4=\alpha_2\left(-\frac{1}{2}-i\frac{\sqrt{3}}{2}\right)$. Таким образом, $g(x)=(x-\alpha_1)(x-\alpha_2)(x-\beta_1)(x-\beta_2)(x-\beta_3)(x-\beta_4)$. Легко видеть, что путем перемножения некоторых из множителей $(x-\alpha_1),(x-\alpha_2),(x-\beta_1),(x-\beta_2),(x-\beta_3),(x-\beta_4)$ нельзя получить многочлен с рациональными коэффициентами, отличный от $g(x)$. Следовательно, $f(x)=g(x)$. ◄

11. Решить в натуральных числах уравнение $x^{2/n}+y^{2/n}=z^{2/n}$.

►Если число n четное, то получаем уравнение вида $x^{1/k}+y^{1/k}=z^{1/k}$, решение которого находили ранее. Пусть n - нечетное. Тогда $x^2=ta^n$, $y^2=tb^n$, $z^2=t(a+b)^n$, где $(a,b)=1$. Тогда $ta=a_1^2, tb=b_1^2, t(a+b)=c_1^2$. Получаем уравнение $a_1^2+b_1^2=c_1^2$. Используя формулы для пифагоровых троек, находим все решения: $(a_1,b_1,c_1)=((p^2-q^2)l,2pql,(p^2+q^2)l)$ или $(a_1,b_1,c_1)=(2pql,(p^2-q^2)l,(p^2+q^2)l)$, где p и q взаимно простые натуральные числа разной четности, $p>q$. Легко установить, что $t=l$. Поэтому $(x,y,z)=((p^2-q^2)^n l,2^n p^n q^n l,(p^2+q^2)^n l)$ или $(x,y,z)=(2^n p^n q^n l,(p^2-q^2)^n l,(p^2+q^2)^n l)$. ◄

12. Найдите наибольшее возможное число шагов алгоритма Евклида с выбором наименьшего по модулю остатка для двух четырехзначных чисел.

► Определим последовательность f_n следующим образом: $f_1=0$, $f_2=1$, $f_{k+2}=2f_{k+1}+f_k$, $k\geq 1$.

Пусть a,b – натуральные взаимно простые числа, $a\geq b$. Пусть алгоритм Евклида с выбором наименьшего по модулю остатка для чисел a,b состоит из $L(a,b)=k$ делений.

Пусть $a=q_1b+r_1$, $b=q_2r_1+r_2$, $r_1=q_3r_2+r_3$,…, $r_{k-3}=q_{k-1}r_{k-2}+r_{k-1}$, $r_{k-2}=q_kr_{k-1}$.

Так как НОД$(r_i, r_{i+1}) = 1$, то $|r_{i+1}| \le \frac{|r_i|}{2}$, причём равенство возможно тогда и только тогда, когда $|r_i| = 2$.

Очевидно, $|r_{k-1}| = 1$. Докажем, что $|q_i| \ge 2$ для любых $i = \overline{2,k}$. Для удобства обозначим $r_0 = b$, $r_k = 0$. Предположим, что найдётся i, такое, что $|q_i| \le 1$. Рассмотрим равенство

$r_{i-2} = q_i r_{i-1} + r_i$. Отсюда получаем, что $|r_{i-2}| \le |q_i||r_{i-1}| + |r_i| \le |r_{i-1}| + |r_i| \le 3|r_i|$, что невозможно, поскольку $|r_{i-2}| \ge 4|r_i|$.

Докажем, что $|r_{i-2}| \ge 2|r_{i-1}| + |r_i|$ для любых $i = \overline{2,k}$.

Допустим, что для некоторого i выполняется неравенство $|r_{i-2}| < 2|r_{i-1}| + |r_i|$. С другой стороны, $r_{i-2} = q_i r_{i-1} + r_i$. Если предположить, что $|q_i| \ge 3$, то получаем, что $|r_{i-2}| \ge 3|r_{i-1}| - |r_i|$. Но тогда $2|r_i| > |r_{i-1}|$, что невозможно. Поэтому $|q_i| = 2$. Для того, чтобы одновременно выполнялись соотношения $|r_{i-2}| < 2|r_{i-1}| + |r_i|$, $r_{i-2} = q_i r_{i-1} + r_i$, необходимо, чтобы числа $q_i r_{i-1}$ и r_i имели разные знаки. Но тогда отсюда, из равенства $r_{i-2} = q_i r_{i-1} + r_i$ и условия $|q_i r_{i-1}| > |r_i|$, получаем, что $|r_{i-2}| < |q_i r_{i-1}| = 2|r_{i-1}|$, что также невозможно. Полученное противоречие доказывает неравенство $|r_{i-2}| \ge 2|r_{i-1}| + |r_i|$ для любых $i = \overline{2,k}$.

Таким образом, $|r_k| = f_1$, $|r_{k-1}| = f_2$, $|r_{k-2}| \ge 2|r_{k-1}| + |r_k| = f_3$, $|r_{k-3}| \ge 2|r_{k-2}| + |r_{k-1}| \ge 2f_3 + f_2 = f_4$,…, $|b| = |r_0| \ge 2|r_1| + |r_2| \ge 2f_k + f_{k-1} = f_{k+1}$.

Докажем, что $a \ge f_{k+1} + f_k$. Предположим противное, т.е. $|a| < f_{k+1} + f_k$. Если предположить, что $|q_1| \ge 2$, то получим, что $|a| \ge 2f_{k+1} - f_k \ge f_{k+1} + f_k$. Поэтому $|q_1| \le 1$. Если $q_1 = 0$, то $|a| = |r_1| < |b|$, что невозможно. Таким образом, $|q_1| = 1$. Если числа $q_1 b$ и r_1 одного знака, то $|a| = |b| + |r_1| \ge f_{k+1} + f_k$. Следовательно, числа $q_1 b$ и r_1 имеют разные знаки, а поскольку, $|b| > |r_1|$, то $|a| = |b| - |r_1| < |b|$. Противоречие. Таким образом, $|a| \ge f_{k+1} + f_k$.

Легко видеть, что в случае когда $a = f_{k+1} + f_k$, $b = f_{k+1}$ выполняется $L(a,b) = k$.

Найдем $N = \max\{k | f_{k+1} + f_k \le 9999\}$. Выпишем первые члены последовательности f_k: 0, 1, 2, 5, 12, 29, 70, 169, 408, 985, 2378, 5741,… Видим, что $N = 11$. ◄