Решения на задачите по теория на числата

Този материал е изготвен със съдействието на школа Sicademy

NT1. Да се реши в цели числа уравнението

$$2^m - 37n^2 = 19.$$

.

Решение. След умножение на двете страни по 4 уравнението може да се запише във вида

$$2(2^{m+1} - 1) = 37((2n)^2 + 2).$$

Тъй като показателят на 2 по модул 37 е 36, то $36|m+1$ и следователно $7 = 2^3 - 1|2^{m+1} - 1$. От друга страна, $7 \nmid (2n)^2 + 2$ за никое $n \in \mathbb{Z}$, откъдето заключаваме, че даденото уравнение няма решение в цели числа.

NT2. Нека p и q са нечетни прости числа, като $q > p$ и

$$A_k = k^{p-1} + k^{p-2} + \cdots + k^2 + k + 1 \quad \text{за} \quad k \in \{1, 2, \ldots, q-1\}.$$

Да се намерят всички възможни остатъци, които могат да се получат при деление на q на числото $A_1 A_2 \cdots A_{q-1}$.

Решение. Ако $q \equiv 1 \pmod{p}$, то $k^p - 1|k^{q-1} - 1$ и сравнението $x^p \equiv 1 \pmod{q}$ има решения в множеството $\{2, 3, \ldots, q-1\}$. Следователно в този случай $A_1 A_2 \ldots A_{q-1} \equiv 0 \pmod{q}$.

Нека $q \not\equiv 1 \pmod{p}$. Тогава $k^p \equiv 1 \pmod{q}$ за $k \in \{2, 3, \ldots, q-1\}$ е невъзможно (Защо?).

Ако $k_1^p \equiv k_2^p \pmod{q}$ за някои $k_1, k_2 \in \{2, 3, \ldots, q-1\}$, $k_1 \neq k_2$. Тогава $(k_1 k_2^{-1})^p \equiv 1 \pmod{q}$, откъдето $k_1 k_2^{-1} \equiv 1 \pmod{q}$ съгласно горното. Тъй като обратният елемент е единствен, получаваме $k_2^{-1} = k_1^{-1}$, т.е. $k_2 = k_1$, противоречие. Следователно остатъците на $k^p - 1$, $k \in \{2, 3, \ldots, q-1\}$, пробягват множеството $\{1, 2, \ldots, q-2\}$, а същото правят и остатъците на $(k-1)^{-1}$, $k \in \{2, 3, \ldots, q-1\}$. Тогава

$$A_2 A_3 \ldots A_{q-1} = \prod_{k=2}^{q-1} (k^p - 1) \prod_{k=2}^{q-1} (k-1)^{-1} \equiv 1 \pmod{q}$$

(използвахме теоремата на Уилсън), откъдето окончателно получаваме

$$A_1 A_2 \ldots A_{q-1} \equiv p \pmod{q}$$

.

NT3. За дадени естествено число n и просто число $p > n$ означаваме с $f_p(n)$ броя на числата от множеството $\{1, 2, \ldots, n\}$, които са квадратични остатъци по модул p. Естественото число n се нарича спокойно по отношение на квадратичните остатъци (споко), ако за всяко просто число $p > n$ имаме $f_p(n) \geq \frac{n}{2}$. Да се определи дали 100 е споко.

Решение. Ще докажем, че 100 не е спокойно по отношение на квадратичните остатъци. За целта е достатъчно да докажем, че $f_p(100) \leq 49$ за някое просто $p > 100$.

Идеята е да изберем просто число p, което е малко по-голямо от 100 и да установим, че квадратичните остатъци в интервала $[101, p-1]$ са повече от половината. Тъй като квадратичните остатъци в $[1, p-1]$ са точно половината, това ще означава, че тези в $[1, 100]$ са по-малко от половината, т.е. $f_p(100) \leq 49$ и значи 100 не е споко.

Числото $p = 109$ има исканите свойства. Директно се проверява, че числата 102, 104, 105, 106 и 108 са квадратични остатъци по модул 109 ($102 \equiv 50^2, 104 \equiv 39^2, 105 \equiv 43^2, 106 \equiv 18^2, 108 \equiv 33^2 \pmod{109}$).