Гимназия 1543, математический спецкурс, 8 В

Занятие 8а: сравнения

Определение. *Решить сравнение* относительно некоторого набора переменных — это значит, найти классы эквивалентности, которым эти переменные принадлежат.

Если говорить более строго, то

Определение. *Решением сравнения* $f(x_1, \dots x_n, a_1, \dots a_m) \equiv 0 \pmod n$ относительно набора переменных x называются соотношения вида $\exists \alpha \in A. x_i \equiv g_i(\alpha, a_1, \dots a_m) \pmod n$, логически эквивалентные исходному сравнению.

Пример. Пусть требуется решить сравнение $x^2 \equiv 1 \pmod 8$. Его решениями (как мы знаем из предыдущего листка) являются

$$x \equiv 1 \pmod 8; \quad x \equiv 3 \pmod 8; \quad x \equiv 5 \pmod 8; \quad x \equiv 7 \pmod 8$$

и только они. Т.е. в данном случае $A = \{1, 2, 3, 4\}$, $g(k) = 2k - 1$.

Замечание. Указанное выше определение, вообще говоря, годится лишь для *полиномиальных* сравнений (в которых f — многочлен). В остальных случаях могут возникать решения, не приводящиеся к вышеуказанному виду (например, множество решений сравнения $|x| \equiv 1 \pmod 3$ невозможно представить в виде объединения классов эквивалентности по модулю 3). В таких случаях в качестве решения сравнения следует привести множество всевозможных значений переменных, удовлетворяющих сравнению.

1) Решите сравнение
   а) $334x \equiv 123 \pmod{1001}$; б) $7x \equiv 2 \pmod{13}$; в) $2x + 3y \equiv 1 \pmod 5$.
2) Решите сравнение
   а) $x^2 + 3x \equiv 15 \pmod{17}$; б) $x^2 + 1533x \equiv 1527 \pmod{1543}$; в) $x^2 + y^2 \equiv 1 \pmod 3$.
3) Решите сравнение (бинарный $x \bmod y$ в пункте в) — операция взятия остатка x по модулю y)
   а) $|x| \equiv 1 \pmod 3$; б) $|x| + |y| \equiv 4 \pmod 5$; в) $x \bmod 5 \equiv 3 \pmod 4$.

Гимназия 1543, математический спецкурс, 8 В

Занятие 8а: сравнения

Определение. *Решить сравнение* относительно некоторого набора переменных — это значит, найти классы эквивалентности, которым эти переменные принадлежат.

Если говорить более строго, то

Определение. *Решением сравнения* $f(x_1, \dots x_n, a_1, \dots a_m) \equiv 0 \pmod n$ относительно набора переменных x называются соотношения вида $\exists \alpha \in A. x_i \equiv g_i(\alpha, a_1, \dots a_m) \pmod n$, логически эквивалентные исходному сравнению.

Пример. Пусть требуется решить сравнение $x^2 \equiv 1 \pmod 8$. Его решениями (как мы знаем из предыдущего листка) являются

$$x \equiv 1 \pmod 8; \quad x \equiv 3 \pmod 8; \quad x \equiv 5 \pmod 8; \quad x \equiv 7 \pmod 8$$

и только они. Т.е. в данном случае $A = \{1, 2, 3, 4\}$, $g(k) = 2k - 1$.

Замечание. Указанное выше определение, вообще говоря, годится лишь для *полиномиальных* сравнений (в которых f — многочлен). В остальных случаях могут возникать решения, не приводящиеся к вышеуказанному виду (например, множество решений сравнения $|x| \equiv 1 \pmod 3$ невозможно представить в виде объединения классов эквивалентности по модулю 3). В таких случаях в качестве решения сравнения следует привести множество всевозможных значений переменных, удовлетворяющих сравнению.

1) Решите сравнение
   а) $334x \equiv 123 \pmod{1001}$; б) $7x \equiv 2 \pmod{13}$; в) $2x + 3y \equiv 1 \pmod 5$.
2) Решите сравнение
   а) $x^2 + 3x \equiv 15 \pmod{17}$; б) $x^2 + 1533x \equiv 1527 \pmod{1543}$; в) $x^2 + y^2 \equiv 1 \pmod 3$.
3) Решите сравнение (бинарный $x \bmod y$ в пункте в) — операция взятия остатка x по модулю y)
   а) $|x| \equiv 1 \pmod 3$; б) $|x| + |y| \equiv 4 \pmod 5$; в) $x \bmod 5 \equiv 3 \pmod 4$.
