Доказательство теоремы **2, b, §2**

Пономарев Николай, 244 группа

Необходимо доказать следующую теорему с помощью средств аксиоматической теории чисел:

Теорема. Если $a = bq + c$, то совокупность общих делителей чисел a и b совпадает с совокупностью общих делителей чисел b и c; в частности, $(a, b) = (b, c)$.

Введем предикатный символ $|$:

Определение 1 (делимость).

$$y \mid x \Leftrightarrow \exists z(x = yz) \tag{1}$$

Тогда на языке аксиоматической теории чисел (**FA**) данная теорема записывается так[1]:

Теорема.

$$\forall x \forall y \forall p \forall q(x = py + q \to \forall z((z \mid x \,\&\, z \mid y \to z \mid q) \,\&\, (z \mid y \,\&\, z \mid q \to z \mid x))) \tag{2}$$

Для доказательства нам потребуется следующая теорема:

Теорема 1 (2, b, §1). Если в равенстве вида $k + l + \dots + n = p + q + \dots + s$ относительно всех членов, кроме какого-либо одного, известно, что они кратны b, то и этот один член кратен b.

Или на языке **FA**:

$$\begin{aligned}\forall w \forall x_1 \dots \forall x_n \forall y_1 \dots \forall y_m \forall z(&z \mid x_1 \,\&\, z \mid x_2 \,\&\, \dots \,\&\, z \mid x_n \,\&\\ &z \mid y_1 \,\&\, z \mid y_2 \,\&\, \dots \,\&\, z \mid y_m \,\&\\ &x_1 + \dots + x_n + w = y_1 + \dots + y_m \to\\ &z \mid w)\end{aligned} \tag{3}$$

Доказательство. Примем без доказательства. ■

Приступим к доказательству теоремы:

Доказательство. Запишем теорему 1 в удобном для нас виде:

$$\forall w \forall x \forall y \forall z(z \mid x \,\&\, z \mid y \,\&\, x = y + w \to z \mid w) \tag{4}$$

Дерево вывода см. далее. Для правил с кванторами условие на то, что переменная или терм свободна для подстановки, считаем выполненным.

Примечания к дереву:

(*) u, v, w, r не входят свободно в заключение правила;

(**) s не входит свободно в заключение правила, т.е. $s \neq u, v, w, r$.

[1]здесь и далее, запись $x \cdot y$ равносильна записи xy; а так же при переходе к языку **FA** будем переименовывать большинство переменных и констант, чтобы соответствовать принятым обозначениям

Аксиомы:

1. при $t_4 = s$ и $t_2 = u$ или $t_4 = s$ и $t_2 = v$;
2. при $t_4 = s$ и $t_3 = u$ или $t_4 = s$ и $t_3 = v$;
3. при $t_2 = u$, $t_3 = wv$ и $t_1 = r$;
4. при $t_4 = s$ и $t_1 = r$;
5. при $t_4 = s$ и $t_2 = v$ или $t_4 = s$ и $t_2 = r$;
6. при $t_4 = s$ и $t_3 = v$ или $t_4 = s$ и $t_3 = r$;
7. при $t_2 = u$, $t_3 = wv$ и $t_1 = r$;
8. при $t_4 = s$ и $t_1 = u$;

$\blacksquare$