## Сравнения по модулю

Зафиксируем натуральное число $m$.

**Определение** Целые числа $a$ и $b$ *сравнимы по модулю* $m$, если $a-b$ делится на $m$.

**Предложение 1** (свойства отношения сравнимости $\mathrm{mod} m$).

(i) $a \equiv a \pmod m$.

(ii) Если $a \equiv b \pmod m$, то $b \equiv a \pmod m$.

(iii) Если $a \equiv b \pmod m$ и $b \equiv c \pmod m$, то $a \equiv c \pmod m$.

Докажите эти утверждения самостоятельно.

**Предложение 2** (арифметические операции над сравнениями). Пусть $a \equiv b \pmod m$, $c \equiv d \pmod m$, $k$ – целое число, $n$ – натуральное число. Тогда

(i) $a+c \equiv b+d \pmod m$ (сравнения можно складывать);

(ii) $a-c \equiv b-d \pmod m$ (сравнения можно вычитать);

(iii) $ka \equiv kb \pmod m$ (сравнения можно умножать на целое число);

(iv) $ac \equiv bd \pmod m$ (сравнения можно перемножать);

(v) $a^n \equiv b^n \pmod m$ (сравнения можно возводить в натуральную степень).

**Доказательство**. По условию $a-b$ и $c-d$ делятся на $m$. Тогда на $m$ делится их сумма $(a-b)+(c-d) = (a+c)-(b+d)$, откуда следует (i); на $m$ делится их разность $(a-b)-(c-d) = (a-c)-(b-d)$, откуда следует (ii); на $m$ делится произведение $k(a-b) = ka-kb$, откуда следует (iii).

Для доказательства (iv) воспользуемся (iii): умножая сравнение $a \equiv b \pmod m$ на $c$, получаем $ac \equiv bc \pmod m$, а умножая сравнение $c \equiv d \pmod m$ на $b$, получаем $bc \equiv bd \pmod m$. Из двух полученных сравнений по предложению 1(iii) следует, что $ac \equiv bd \pmod m$.

Наконец, (v) получается, если перемножить $n$ одинаковых сравнений $a \equiv b \pmod m$.