

СРАВНЕНИЕ ПО МОДУЛЮ

Утверждение		Пояснение/ доказательство
Определение сравнения по модулю	Если два числа * a и b при делении на натуральное число n дают один и тот же остаток r , то такие числа называются сравнимыми по модулю n .	$a = nq_1 + r;$ $b = nq_2 + r$ $a \equiv b \pmod{n}$
Следствие из определения сравнения по модулю	Два числа a и b сравнимы по модулю n тогда и только тогда, когда $a-b$ делится на n .	$a \equiv b \pmod{n} \Leftrightarrow$ $\Leftrightarrow a - b = q_3 n$
	2.1 Если два числа a и b сравнимы по модулю n , то $a-b$ делится на n .	$a = nq_1 + r;$ $b = nq_2 + r$ $a - b = n(q_1 - q_2) = q_3 n$
	2.2 Если разность двух чисел a и b делится на n , то эти числа сравнимы по модулю n .	$a = nq_1 + r_1; b = nq_2 + r_2$ $a - b = n(q_1 - q_2) + r_1 - r_2$ <p>По утверждению $a-b$ делится на n. Следовательно $r-r_1$ тоже делится на n. Но т.к. r и r_1 числа $0, 1, \dots, n-1$, то абсолютное значение $r-r_1 < n$. Тогда, для того, чтобы $r-r_1$ делился на n должно выполняться условие $r=r_1$.</p> <p>Из утверждения следует, что сравнимые числа - это такие числа, разность которых делится на модуль.</p>
Свойство 1. рефлексивности	Для любого целого a и натурального n всегда $a \equiv a \pmod{n}$.	
Свойство 2. симметричности :	Для любого целого a и натурального n всегда $a \equiv b \pmod{n} \Leftrightarrow b \equiv a \pmod{n}$	$a \equiv b \pmod{n} \Leftrightarrow a - b = qn \Leftrightarrow$ $b - a = q_1 n \Leftrightarrow$ $\Leftrightarrow b \equiv a \pmod{n}$
Свойство 3. транзитивности:	Если два числа a и c сравнимы с числом b по модулю n , то a и c сравнимы между собой по тому же модулю, т.е. если $a \equiv b \pmod{n}, b \equiv c \pmod{n}$, то $a \equiv c \pmod{n}$.	Из условия свойства 2 следует $a-b$ и $b-c$ делятся на n . Тогда их сумма $a-b+(b-c)=a-c$ также делится на n .
Свойство 4. (сложение сравнений)	Если $a \equiv b \pmod{n}$ и $m \equiv p \pmod{n}$, то $a+m \equiv b+p \pmod{n}$ и $a-m \equiv b-n \pmod{n}$.	<p>Так как $a-b$ и $m-p$ делятся на n, то $(a-b)+(m-p)=(a+m)-(b+p)$, $(a-b)-(m-p)=(a-m)-(b-n)$ также делятся на p.</p> <p>Это свойство можно распространить на какое угодно число сравнений, имеющих один и тот же модуль (доказательство можно провести по мми).</p>
Свойство 5. (умножение сравнений)	Если $a \equiv b \pmod{n}$ и $m \equiv p \pmod{n}$, то $am \equiv bp \pmod{n}$.	<p>Так как $a-b$ делится на n, то $(a-b)m$ также делится на n, следовательно, $am \equiv bm \pmod{n}$. Далее $m-p$ делится на n, следовательно, $b(m-p)=bm-bp$ также делится на n, значит $bm \equiv bp \pmod{n}$.</p> <p>Таким образом два числа am и bp сравнимы по модулю с одним и тем же числом bm, следовательно они сравнимы между собой (свойство 3).</p>

Свойство 6. (возведение сравнения в степень)	Если $a \equiv b \pmod{n}$, то $a^k \equiv b^k \pmod{n}$, где k некоторое неотрицательное целое число.	следует из свойства 4 и ММИ
Замечание (деление сравнений)	При делении все обстоит иначе. Из сравнения $am \equiv bm \pmod{n}$ не всегда следует сравнение $a \equiv b \pmod{n}$.	Примеры:
Свойство 7. (деление сравнений)	Пусть $am \equiv bm \pmod{n}$, тогда $a \equiv b \pmod{n/\lambda}$, где λ это <u>наибольший общий делитель</u> чисел m и n .	Пусть λ наибольший общий делитель чисел m и n . Тогда $m = m_1 \lambda$ и $n = n_1 \lambda$. Так как $m(a-b)$ делится на n , то $\frac{m(a-b)}{n} \in \mathbb{Z}$. Тогда $\frac{m(a-b)}{n} = \frac{m_1 \lambda (a-b)}{n_1 \lambda} = \frac{m_1 (a-b)}{n_1}$. Следовательно, $\frac{m_1 (a-b)}{n_1}$ имеет нулевой остаток, т.е. $m_1 (a-b)$ делится на n_1 . Но числа m_1 и n_1 взаимно простые. Следовательно $a-b$ делится на $n_1 = n/\lambda$ и, тогда, $a \equiv b \pmod{n/\lambda}$.
Свойство 8. (сравнение по делителю модуля)	Если $a \equiv b \pmod{n}$ и m является одним из делителей числа n , то $a \equiv b \pmod{m}$.	$a-b$ делится на n . n делится на m . Следовательно $a-b$ делится на m .
Свойство 9. (сравнение по составному модулю)	Если $a \equiv b \pmod{p}$, $a \equiv b \pmod{q}$, $a \equiv b \pmod{s}$, то $a \equiv b \pmod{h}$, где h наименьшее общее кратное чисел p, q, s .	Разность $a-b$ должна быть числом, кратным p, q, s . и, следовательно, должна быть кратным h . В частном случае, если модули p, q, s взаимно простые числа, то $a \equiv b \pmod{h}$, где $h = pqs$.



Модульная арифметика, часто называемая модулярной арифметикой, широко применяется в [математике](#), [информатике](#) и [криптографии](#).

