Арифметика остатков

группа «Бресква»

Определение.

Если $a - b \vdots m$, то говорят, что a и b *сравнимы по модулю* m. Сравнимость записывают так: $a \equiv b \pmod{m}$.

Иными словами, a и b сравнимы по модулю m, если они дают одинаковые остатки при делении на m.

1. Докажите, что если $a \equiv b \pmod{m}$ и $c \equiv d \pmod{m}$, то
   а) $a + c \equiv b + d \pmod{m}$; б) $ac \equiv bd \pmod{m}$.
2. Докажите, что если $a \equiv b \pmod{m}$ и k — натуральное число, то $a^k \equiv b^k \pmod{m}$.
3. Постройте таблицу умножения по модулю 5.
4. Постройте таблицу умножения по модулю 6.
5. Найдите наименьшие неотрицательные остатки $6^k+1 \pmod{17}$ при $k = 1, 2, 3, 4, 5$.
6. Пусть $d \perp m$ и $ad \equiv bd \pmod{m}$. Тогда $a \equiv b \pmod{m}$. Докажите.
7. Пусть d — натуральное число, являющееся общим делителем a, b и m. Докажите, что сравнения $a \equiv b \pmod{m}$ и $a/d \equiv b/d \pmod{m/d}$ равносильны.
8. Докажите, что $7^{2014} + 9^{2014} \vdots 10$.
9. Докажите, что ни при каком натуральном n число $3^n + 5^n$ не является полным квадратом.
10. Пусть x, y, z — целые числа, удовлетворяющие уравнению $x^2+y^2 = z^2$. Докажите, что $xyz \equiv 0 \pmod{60}$.
11. Найдите остатки от деления 100^{125}...
    а) ... на 99; б) ... на 101; в) ... на 9999.
12. Найдите отстаток от деления числа $2011 \cdot 2012 \cdot 2013 \cdot 2014 \cdot 2015$...
    а) ... на 2010; б) ... на 2016.
13. Докажите, что 2^{100} и 3^{100} сравнимы...
    а) ... по модулю 5; б) ... по модулю 13.
14. Докажите, что $2^{5n+1} + 5^{n+2} \vdots 27$.

Решение сравнений

группа «Бресква»

1. Пусть $d = \text{НОД}(c, b)$. Докажите, что любое x такое, что $x \equiv c \pmod b$, делится на d, то есть $x \equiv 0 \pmod d$, и при этом $x/d \equiv c/d \pmod{b/d}$.
2. Пусть b – нечётное число и $2ax \equiv 2c \pmod b$. Докажите, что $ax \equiv c \pmod b$.
3. Пусть $\text{НОД}(b, k) = 1$. Докажите, что сравнение $kax = kc \pmod b$ можно сократить на k: из $kax \equiv kc \pmod b$ следует, что $ax \equiv c \pmod b$.
4. Докажите, что если $d = \text{НОД}(a, b) > 1$, то сравнение $ax \equiv 0 \pmod b$ имеет ненулевое решение.

   Определение.
   Остаток $a \pmod b$ назовём *обратимым*, если существует *обратный* к нему остаток, то есть такой a', для которого $aa' \equiv 1 \pmod b$. Для обозначения a' будем использовать $1/a$.

5. а) Докажите, что если $\text{НОД}(a, b) = 1$, то остаток a обратим.
   б) Докажите, что если остаток $a \pmod b$ обратим, то $\text{НОД}(a, b) = 1$.
   в) Докажите, что если $\text{НОД}(a, b) = 1$, то решением сравнения $ax \equiv c \pmod b$ является $c/a \pmod b$, то есть $c \cdot (1/a)$.
6. Найдите все решения сравнений:
   а) $4x \equiv 9 \pmod{13}$;
   б) $3x \equiv 12 \pmod{15}$;
   в) $20x \equiv 30 \pmod{55}$.
7. Решите систему сравнений

$$\begin{cases} 6x + 5y \equiv 1 \pmod{11}, \\ 4x + 3y \equiv 2 \pmod{11}. \end{cases}$$

Китайская теорема об остатках

Китайская теорема об остатках.

Пусть $n_1, n_2, \dots n_k$ — натуральные попарно взаимно простые числа, а $r_1, \dots, r_k$ — некоторые целые числа. Тогда существует такое целое число M, что оно будет решением системы сравнений:

$$\begin{cases} M \equiv r_1 \pmod{n_1} \\ M \equiv r_2 \pmod{n_2} \\ \quad \dots \\ M \equiv r_k \pmod{n_k} \end{cases}$$

Введём обозначение $N = n_1 \cdot \ldots \cdot n_k$, $N_i = \dfrac{N}{n_i}$. Определим M_i как $M_i N_i \equiv 1 \pmod{m_i}$. Явная формула для M:

$$M = r_1 M_1 N_1 + r_2 M_2 N_2 + \ldots + r_k M_k N_k$$

1. Найдите
   а) $3^{-1} \pmod 7$;
   б) $7^{-1} \pmod 3$.
2. Какие цифры следует поставить вместо звёздочек, чтобы число $454{*}{*}$ делилось на 2, 7 и 9?
3. Олег собрал мешочек монет. Саша пересчитал их, и оказалось, что если разделить все монеты на пять равных кучек, то останется две лишние монеты. А если на четыре равные кучки — останется одна лишняя монета. В то же время монетки можно разделить на три равные кучки. Какое наименьшее число монет могло быть у Олега?
4. Найдите наименьшее натуральное число, дающее при делении на 2, 3, 5, 7 остатки 1, 2, 4, 6 соответственно.
5. Укажите все целые числа x, удовлетворяющие системам
   а) $\begin{cases} x \equiv 3 \pmod{5} \\ x \equiv 7 \pmod{17} \end{cases}$
   б) $\begin{cases} x \equiv 2 \pmod{13} \\ x \equiv 4 \pmod{19} \end{cases}$
6. При каких целых n число $n^2 + 3n + 1$ делится на 55?