## Дроби по модулю. 20 июня

Всё по модулю некоторого натурального числа $m$, большего 1.

**Определение.** *Вычетом* по модулю $m$ будем называть все числа, дающие фиксированный остаток при делении на $m$. Вычет, которому принадлежит число $a$ (временно) обозначим $[a]$.

**Определение.** Определим $[a]+[b]$ как $[a+b]$, а $[a]\cdot[b]$ как $[ab]$.

**Утверждение.** Введённые операции корректно определены, т.е. если $[a_1]=[a_2]$, $[b_1]=[b_2]$, то $[a_1+b_1]=[a_2+b_2]$ и $[a_1b_1]=[a_2b_2]$. Другими словами, не важно, какого именно представителя некоторого вычета мы возьмём, результат сложения и умножения от этого не изменится.

**Осознание.** У нас было утверждение «если $a\equiv b \pmod m$, то $P(a)\equiv \equiv P(b) \pmod m$». Я про него говорил, что оно должно быть очевидным. По сути тут сказано, что если $[a]=[b]$, то $[P(a)]=[P(b)]$ — это легко видеть из утверждения выше.

**Комментарий.** Дальше мы будем везде опускать квадратные скобки, обозначая $[a]$ просто как $a$.

**Утверждение.** Пусть $s$ – вычет по модулю $m$, $(s,m)=1$ (*почему так можно писать?*). Тогда существует целое число $t$, что $st\equiv 1 \pmod m$. Более того, любые два таких $t$ сравнимы по модулю $m$, т.е. по сути $t$ — вычет.

**Определение.** Вычет из утверждения выше называют вычетом, *обратным к $s$ по модулю $m$*, и обозначают $s^{-1}$.

**Обозначение.** Через $\frac{a}{b}$ обозначим вычет, равный $a\cdot b^{-1}$.

**Утверждение.** Дроби по модулю можно складывать и вычитать, умножать и делить, сокращать. Более того, если $\frac{a}{b}$ — целое число и $(b,m)=1$, то $\frac{a}{b}\equiv\frac{a}{b}$.

**Комментарий.** Число $\frac{n(n+1)}{2}$ всегда целое. Однако смотреть на него как на дробь по модулю 2 (или другое чётное число) нельзя. Подставьте $n=1$ и $n=3$ (которые сравнимы по модулю 2) и получатся разные по модулю 2 числа.

**Вопрос.** Нельзя, но если очень хочется, то можно. По какому модулю должны быть сравнимы числа $n_1$ и $n_2$, чтобы числа $\frac{n_1(n_1+1)}{2}$ и $\frac{n_2(n_2+1)}{2}$ были сравнимы по модулю 16?

*Задачи на другой стороне!*

«Сириус», Эйлеровская математическая программа 2023, Э2–Э3

Дроби по модулю. 20 июня

Всё по модулю некоторого натурального числа $m$, большего 1.

**Определение.** *Вычетом* по модулю $m$ будем называть все числа, дающие фиксированный остаток при делении на $m$. Вычет, которому принадлежит число $a$ (временно) обозначим $[a]$.

**Определение.** Определим $[a]+[b]$ как $[a+b]$, а $[a]\cdot[b]$ как $[ab]$.

**Утверждение.** Введённые операции корректно определены, т.е. если $[a_1]=[a_2]$, $[b_1]=[b_2]$, то $[a_1+b_1]=[a_2+b_2]$ и $[a_1b_1]=[a_2b_2]$. Другими словами, не важно, какого именно представителя некоторого вычета мы возьмём, результат сложения и умножения от этого не изменится.

**Осознание.** У нас было утверждение «если $a\equiv b \pmod m$, то $P(a)\equiv \equiv P(b) \pmod m$». Я про него говорил, что оно должно быть очевидным. По сути тут сказано, что если $[a]=[b]$, то $[P(a)]=[P(b)]$ — это легко видеть из утверждения выше.

**Комментарий.** Дальше мы будем везде опускать квадратные скобки, обозначая $[a]$ просто как $a$.

**Утверждение.** Пусть $s$ – вычет по модулю $m$, $(s,m)=1$ (*почему так можно писать?*). Тогда существует целое число $t$, что $st\equiv 1 \pmod m$. Более того, любые два таких $t$ сравнимы по модулю $m$, т.е. по сути $t$ — вычет.

**Определение.** Вычет из утверждения выше называют вычетом, *обратным к $s$ по модулю $m$*, и обозначают $s^{-1}$.

**Обозначение.** Через $\frac{a}{b}$ обозначим вычет, равный $a\cdot b^{-1}$.

**Утверждение.** Дроби по модулю можно складывать и вычитать, умножать и делить, сокращать. Более того, если $\frac{a}{b}$ — целое число и $(b,m)=1$, то $\frac{a}{b}\equiv\frac{a}{b}$.

**Комментарий.** Число $\frac{n(n+1)}{2}$ всегда целое. Однако смотреть на него как на дробь по модулю 2 (или другое чётное число) нельзя. Подставьте $n=1$ и $n=3$ (которые сравнимы по модулю 2) и получатся разные по модулю 2 числа.

**Вопрос.** Нельзя, но если очень хочется, то можно. По какому модулю должны быть сравнимы числа $n_1$ и $n_2$, чтобы числа $\frac{n_1(n_1+1)}{2}$ и $\frac{n_2(n_2+1)}{2}$ были сравнимы по модулю 16?

*Задачи на другой стороне!*

**1.** Докажите, например, что если

$$\frac{a_1}{b_1} \equiv \frac{a_2}{b_2} \equiv \frac{a_3}{b_3} \pmod m, \text{ то } \frac{a_1}{b_1} \equiv \frac{a_1 + 2a_2 + 3a_3}{b_1 + 2b_2 + 3b_3} \pmod m.$$

Естественно, в предположении, что все дроби определены.

**2.** Посмотрим на выражение

$$\frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1}.$$

a) Докажите, что после сложения числитель суммы делится на $p$. *По детски, без использования дробей по модулю, а разбивая на пары.*
b) Посмотрим на это выражение как на дроби по модулю. Что здесь написано? Почему пункт a) стал очевиден?

**Комментарий.** Помимо некоторого технического удобства, дроби по модулю дают новые способы «естественного» упорядочивания вычетов. Например, $\frac{1}{1}$, $\frac{1}{2}$, $\ldots$, $\frac{1}{p-1}$, из задачи выше.

**3.** Докажите, что если простое число $p \neq 3$ является делителем числа вида $a^2 + 9$, то $p$ является делителем какого-то числа вида $c^2 + 1$.

**4.** Пусть $a$, $b$, $x$, $y$ и $n$ — натуральные числа. Известно, что каждое из чисел $ax - 1$, $by - 1$ и $x + y - 1$ делится на $n$. Докажите, что $ab - a - b$ также делится на $n$.

**5.** Докажите, что для кажого простого $p$ существует натуральное $n$ такое, что $2^n + 3^n + 6^n \equiv 1 \pmod p$.

**6.** Пусть $p$ — простое. Докажите, что существует такая перестановка $(x_1, x_2, \ldots, x_{p-1})$ чисел $(1, 2, \ldots, p-1)$, что

$$x_1x_2 + x_2x_3 + \ldots + x_{p-2}x_{p-1} \equiv 2 \pmod p.$$

**7.** Докажите, что для каждого простого $p$ числа от 1 до $p - 1$ можно выписать в ряд $a_1, a_2, \ldots, a_{p-1}$ так, что все произведения $a_1a_2 \ldots a_k$ различны по модулю $p$.

**1.** Докажите, например, что если

$$\frac{a_1}{b_1} \equiv \frac{a_2}{b_2} \equiv \frac{a_3}{b_3} \pmod m, \text{ то } \frac{a_1}{b_1} \equiv \frac{a_1 + 2a_2 + 3a_3}{b_1 + 2b_2 + 3b_3} \pmod m.$$

Естественно, в предположении, что все дроби определены.

**2.** Посмотрим на выражение

$$\frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1}.$$

a) Докажите, что после сложения числитель суммы делится на $p$. *По детски, без использования дробей по модулю, а разбивая на пары.*
b) Посмотрим на это выражение как на дроби по модулю. Что здесь написано? Почему пункт a) стал очевиден?

**Комментарий.** Помимо некоторого технического удобства, дроби по модулю дают новые способы «естественного» упорядочивания вычетов. Например, $\frac{1}{1}$, $\frac{1}{2}$, $\ldots$, $\frac{1}{p-1}$, из задачи выше.

**3.** Докажите, что если простое число $p \neq 3$ является делителем числа вида $a^2 + 9$, то $p$ является делителем какого-то числа вида $c^2 + 1$.

**4.** Пусть $a$, $b$, $x$, $y$ и $n$ — натуральные числа. Известно, что каждое из чисел $ax - 1$, $by - 1$ и $x + y - 1$ делится на $n$. Докажите, что $ab - a - b$ также делится на $n$.

**5.** Докажите, что для кажого простого $p$ существует натуральное $n$ такое, что $2^n + 3^n + 6^n \equiv 1 \pmod p$.

**6.** Пусть $p$ — простое. Докажите, что существует такая перестановка $(x_1, x_2, \ldots, x_{p-1})$ чисел $(1, 2, \ldots, p-1)$, что

$$x_1x_2 + x_2x_3 + \ldots + x_{p-2}x_{p-1} \equiv 2 \pmod p.$$

**7.** Докажите, что для каждого простого $p$ числа от 1 до $p - 1$ можно выписать в ряд $a_1, a_2, \ldots, a_{p-1}$ так, что все произведения $a_1a_2 \ldots a_k$ различны по модулю $p$.