Обратные остатки

Общая интуиция.
В этом листочке речь идет о **простом модуле** p!

Вы умеете складывать, вычитать и умножать остатки на друг друга, получая другие остатки. Единственное, чего не хватает для схожести с "обычными" числами — это умение делить любой остаток на любой ненулевой.

Оказывается, можно и дробям довольно естественным образом сопоставить остатки! Причем при любых арифметических действиях с дробями остатки будут вести себя так же (при сложении складываться, при умножении умножаться и т.д.).

1. Дано простое число p и его ненулевой остаток a.
(а) Докажите, что в последовательности $a \cdot 1, a \cdot 2, \dots a \cdot (p-1)$ все остатки разные.
(б) Докажите, что существует единственный остаток b, такой что $ab \underset{p}{\equiv} 1$.

Такой остаток называется обратным остатком для a.

Мораль
Можно ввести понятие остатка или сравнений по модулю для дробей, у которых знаменатель не кратен p:

$$\frac{m}{a} \underset{p}{\equiv} m \cdot b, \quad \text{где } b \text{ — обратный остаток } a.$$

П(р)оверьте, что определение действительно корректное:
— остаток дроби не меняется с выбором другой записи той же дроби;
— сумма дробей дает такой же остаток, что и сумма остатков этих дробей (и так со всеми арифм. действиями).

2. **(а)** Какие остатки совпадают со своими обратными остатками?
(б) **(Теорема Вильсона)** Докажите, что для простого p выполнено $(p-1)! \underset{p}{\equiv} -1$.

3. В Москве каждую секунду один из жителей ест печеньку. Доказать, что если собрать все печеньки, съеденные за 6 недель и одну секунду, то их можно разделить на 11 равных кучек.

4. Докажите через обратные остатки, что m делится на 101, если: $\frac{1}{1} + \frac{1}{2} + \dots + \frac{1}{100} = \frac{m}{n}$.

5. **(а)** На доске написаны числа $\frac{100}{1}, \frac{99}{2} \dots \frac{1}{100}$. Можно ли выбрать какие-то пять из них,

произведение которых равняется единице?

(б) Пусть произведение каких-то $2k+1$ чисел, написанных на доске, равно $\frac{m}{n}$. Докажите, что $m \underset{101}{\equiv} -n$.

6. Докажите, что для простого q выражение $(2q-1)! - q$ делится на q^2.