Теория чисел

Напомню, что происходило на занятии. Вначале мы определили функцию Эйлера $\varphi(n)$. Установили, что $\varphi(p^k) = p^k - p^{k-1}$, где p – простое, затем доказали, что если $(a, b) = 1$, то $\varphi(ab) = \varphi(a)\varphi(b)$. Затем отсюда мы вывели, что

$$\varphi(p_1^{\alpha_1} \cdot ... \cdot p_k^{\alpha_k}) = \varphi(p_1^{\alpha_1}) \cdot ... \cdot \varphi(p_k^{\alpha_k}) = \prod_{i=1}^{k} \left(p_i^{\alpha_i} - p^{\alpha_i - 1}\right),$$

где p_i – простые. Дальше –

Теорема Эйлера. $a^{\varphi(m)} \equiv 1 (\mathrm{mod}\, m)$, *если* $(a, m) = 1$.

Из неё очевидным образом следует

Малая теорема Ферма. $a^{p-1} \equiv 1 (\mathrm{mod}\, p)$, *когда* $(a, p) = 1$ *и* $p \in \mathbb{P}$.

Была у нас и

Теорема Вильсона. *Если* p *– простое, то* $(p-1)! + 1$ *делится на* p.

Остановились мы на обсуждении квадратичных вычетов по простым модулям. Число a называется *квадратичным вычетом* по модулю p, если существует такое целое число x, что $x^2 \equiv a(p)$. В противном случае a называется *квадратичным невычетом*. Данный факт кодируется с помощью так называемого *символа Лежандра*:

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & \text{если } a \vdots p \\ 1, & \text{если } a - \text{квадратичный вычет} \\ -1, & \text{иначе} \end{cases}$$

Очевидно, что если $a_1 \equiv a_2(p)$, то $\left(\frac{a_1}{p}\right) = \left(\frac{a_2}{p}\right)$.

Рассмотрим систему остатков:

$$-\frac{p-1}{2}, ..., -2, -1, 0, 1, 2, ..., \frac{p-1}{2}.$$

Среди них участвуют все представители остатков, поскольку если прибавить к отрицательным остаткам p мы получим

$$\frac{p+1}{2}, ..., p-1,$$

т. е. получим все остатки от 0 до $p-1$. Кроме того, в этой последовательности содержится $(p-1)/2$ вычетов и столько же невычетов. Действительно, повозводим в квадрат остатки этой системы, получим:

$$1^2, 2^2, ..., \left(\frac{p-1}{2}\right)^2.$$

Пусть r_1^2 и r_2^2, $1 \leqslant r_1, r_2 \leqslant (p-1)/2$ – два различных числа из этой последовательности. Тогда $r_1^2 - r_2^2 = (r_1 - r_2)(r_1 + r_2)$ не делится на p, поскольку $r_1 + r_2 < p$ и $|r_1 - r_2| < p$, поэтому эти квадраты дают разные остатки при делении на p, поэтому и вычетов всего $(p-1)/2$, остальные $(p-1)/2$ – невычеты.

Задача 1. Докажите, что если a – квадратичный вычет по модулю p, то $a^{(p-1)/2} \equiv 1(p)$. Если a – квадратичный невычет, то $a^{(p-1)/2} \equiv -1(p)$.

Задача 2. Докажите, что сравнение $x^n \equiv a(p)$ имеет не более n решений.

Пусть теперь $a^{(p-1)/2} \equiv 1(p)$. Заметим, что этому соотношению в силу задачи 1 удовлетворяют все квадратичные вычеты. Тогда согласно задаче 2 ничего не остаётся, кроме как быть числу a квадратичным вычетом по модулю p. Аналогично проходят рассуждения и в случае минус единицы. Таким образом, доказано

Утверждение. $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2}(p)$.

Задача 3. Докажите, что если n^2+1 делится на нечётное простое p, то $p = 4k+1$.

Задача 4. Докажите, что $\left(\frac{a_1 a_2 ... a_n}{p}\right) = \left(\frac{a_1}{p} ... \frac{a_n}{p}\right)$.

Задача 5. Выпишем в ряд все правильные дроби со знаменателем n и сделаем возможные сокращения. Например, для $n = 12$ получится следующий ряд:

$$\frac{0}{1}, \frac{1}{12}, \frac{1}{6}, \frac{1}{4}, \frac{1}{3}, \frac{5}{12}, \frac{1}{2}, \frac{7}{12}, \frac{2}{3}, \frac{3}{4}, \frac{5}{6}, \frac{11}{12}.$$

Сколько получится дробей со знаменателем d, если d – некоторый делитель n.

Задача 6. Докажите, что

$$\sum_{d|n} \varphi(d) = n.$$

Задача 7. Докажите, что длина периода десятичной дроби $1/p$ делит $p-1$.

Задача 8. Докажите, что число 11...1, в записи которого участвуют $p-1$ единиц, делится на простое $p \geqslant 7$.

Задача 9. Найдите остаток от деления числа 5^{2018} на 43.