# Малая теорема Ферма (лекция).

**1. Напоминание.** Все числа в этой лекции натуральные или 0. Мы помним из прошлогоднего курса, что любое число на любое ненулевое можно однозначно поделить с остатком: $a = bk + r$, где $a$ — делимое, $b$ — делитель, $k$ — неполное частное, а $0 \leqslant r < b$ — остаток от деления $a$ на $b$. Мы говорили, что $m$ и $n$ сравнимы по модулю $l$ (пишется $m \equiv n\,(mod\,l)$), если $m$ и $n$ дают одинаковые остатки при делении на $l$ или, что то же самое, если $(m-n)\vdots l$. Мы знаем, что при сложении, вычитании и умножении чисел их остатки по данному модулю тоже складываются, вычитаются и умножаются, а потому можно заниматься арифметикой остатков. Например, по модулю 7 верно: $4+6=3$, $4-6=5$, $4\cdot 6=3$ и так далее. Множество всех остатков по модулю $n$ обозначается $\mathbb{Z}_n$. Несколько раз нам понадобится известная важная лемма: если $ab\vdots c$ и $НОД(a\,;\,c)=1$, то $b\vdots c$.

**2. Деление.** Разберём вопрос о делении остатков. Раз уж $4\cdot 6 = 3(mod\,7)$, насколько оправданно считать, что $3:6 = 4(mod\,7)$? Вообще говоря, так рассуждать нельзя: например по модулю 6 окажется, что $3:3=1$, $3:3=3$ и $3:3=5$ одновременно. Наоборот, $3:2$ вообще не существует. Однако по простому модулю деление (не на 0) возможно и однозначно.

В самом деле, пусть $p$ — простое число. Рассмотрим отображение $f:\mathbb{Z}_p \longrightarrow \mathbb{Z}_p$, заданное так: $f(x)=ax$, где $a$ — фиксированный ненулевой элемент $\mathbb{Z}_p$. Покажем, что это биекция. Инъективность доказывается от противного: если $f(x)=f(y)$, то $ax=ay$, то есть $(ax-ay)\vdots p$, а тогда $a(x-y)\vdots p$, но поскольку $НОД(a\,;\,p)=1$, то $x=y$. Заметим, что мы по сути "сократили" на $a$: от $ax=ay$ перешли к $x=y$. Сюръективность следует из того, что образы всех элементов различны, то есть их ровно $p$, но в $\mathbb{Z}_p$ ровно столько элементов, так что все элементы служат образами.

Раз $f$ биекция, деление возможно: в качестве частного от деления $c$ на $a$ берут прообраз $c$ при отображении $f$.

В дальнейшей части лекции все равенства будут пониматься по некоторому простому модулю $p$.

**3. Малая теорема Ферма.** Поскольку $f:\mathbb{Z}_p \longrightarrow \mathbb{Z}_p$ — биекция, множества $\{0\,;\,1\,;\,2\,;\,3\,\ldots\,p-2\,;\,p-1\}$ и $\{a\cdot 0\,;\,a\cdot 1\,;\,a\cdot 2\,;\,a\cdot 3\,\ldots\,a\cdot(p-2)\,;\,a\cdot(p-1)\}$ совпадают, а тогда равны и произведения ненулевых элементов в них. То есть $1\cdot 2\cdot 3\ldots\cdot(p-1)=(1\cdot a)\cdot(2\cdot a)\cdot(3\cdot a)\ldots\cdot((p-1)\cdot a)$, откуда $(p-1)!=a^{p-1}\cdot(p-1)!$. Поскольку $(p-1)!$ взаимно просто с $p$, то $a^{p-1}=1$. Это и есть малая теорема Ферма. Она утверждает, что $\boxed{\text{если } a \text{ не кратно простому } p, \text{ то } a^{p-1}=1(mod\,p)}$.

**4. Набросок другого доказательства.** Как мы знаем, $C_p^k \vdots p$ при всех $k$, кроме 0 и $p$. Поэтому в силу бинома Ньютона $(a+1)^p = a^p+1$. То есть, при увеличении основания степени на 1, степень тоже растёт на 1. При $a=1$ имеем $1^p=1$, так что $a^p=a$, а тогда $a^{p-1}=1$.

**5. Несколько примеров.** Какой остаток при делении на 101 даёт число $7^{100}$? А $7^{104}$? А $7^{99}$? На первый вопрос ответ 1, на второй вопрос ответим так: $7^{104}=7^{100}\cdot 7^4$, так что остаток 78. Для ответа на третий вопрос потребуется найти такой остаток $x$, чтобы $7x=1$. Остаток $x$ можно подобрать, но лучше воспользоваться техникой решения диофантовых уравнений. Ведь мы ищем такой $x$, чтобы $7x-101k=1$. Если его решить, припомнив обратный алгоритм Евклида, получится, что $x=29$.

Разберём ещё такую задачу: докажите, что число $111\ldots1$ (2002 единицы) делится на 2003. В самом деле, число 2003 простое, поэтому по МТФ $10^{2002}-1$ делится на 2003. Но это число равно данному в условии, умноженному на 9, поэтому задача решена.