# Малая теорема Ферма

*В.СЕНДЕРОВ, А.СПИВАК*

МЫ РАССКАЖЕМ О ПЕРИОДИЧНОСТИ ОСТАТКОВ (заново доказав малую теорему Ферма и теорему Эйлера в формулировках, которые позволят решить многие интересные задачи), о первообразных корнях, функции Кармайкла, числах Мерсенна и о многом другом.

Статья насыщена интересными задачами. Вряд ли возможно при первом чтении решить их все. Но мы уверены: многие из них настолько заинтригуют вас, что рано или поздно все они будут решены – самостоятельно или с помощью раздела «Ответы, указания, решения».

### Напоминание

Как помнит читатель первой части статьи, числа $a$ и $b$ сравнимы по модулю $n$, если $a-b$ кратно $n$, т.е. $a-b=kn$, где $k$ – целое число.

*Продолжение. Начало см. в «Кванте» №1*

**Малая теорема Ферма** гласит: $a^p \equiv a \pmod p$ для любого целого числа $a$ и простого числа $p$. В частности, если $a$ не кратно $p$, то $a^{p-1} \equiv 1 \pmod p$.

**Функция Эйлера** $\varphi(n)$ – это количество взаимно простых с числом $n$ и не превосходящих $n$ натуральных чисел. Например, $\varphi(p)=p-1$ для любого простого $p$. В первой части для $n=p_1^{m_1}p_2^{m_2}\cdot\ldots\cdot p_s^{m_s}$, где $p_1, p_2, \ldots, p_s$ – различные простые числа, $m_1, m_2, \ldots, m_s$ – натуральные числа, доказана общая формула

$$\varphi(n)=\varphi\left(p_1^{m_1}\right)\varphi\left(p_2^{m_2}\right)\cdot\ldots\cdot\varphi\left(p_s^{m_s}\right)=$$

$$=\left(p_1^{m_1}-p_1^{m_1-1}\right)\left(p_2^{m_2}-p_2^{m_2-1}\right)\cdot\ldots\cdot\left(p_s^{m_s}-p_s^{m_s-1}\right).$$

**Теорема Эйлера** – это обобщение малой теоремы Ферма на случай составного модуля: $a^{\varphi(n)} \equiv 1 \pmod n$, где $a$ – целое число, взаимно простое с натуральным числом $n$.

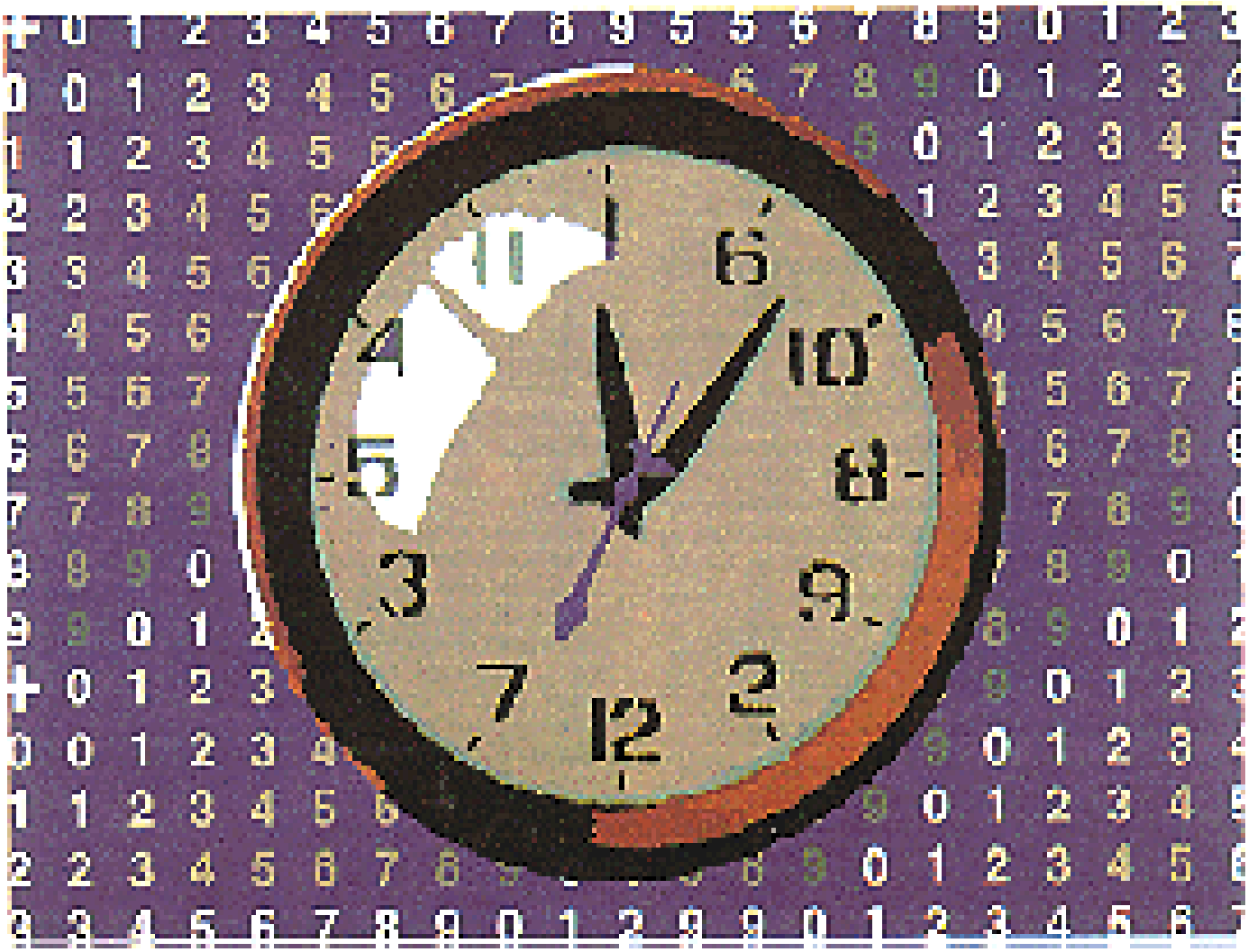

*Иллюстрация М.Сумниной*