Примеры на делимость

Функция Эйлера. Для каждого $n \in \mathbb{Z}$ обозначим через $\varphi(n)$ *функцию Эйлера* — число обратимых элементов кольца $\mathbb{Z}/n\mathbb{Z}$ (т. е. количество всех взаимно простых с n чисел $k \in \mathbb{N}$, не превосходящих $n-1$).

А4-1. Докажите, что функция Эйлера является мультипликативным характером[1], и что если $m = p_1^{k_1} \cdot \dots \cdot p_n^{k_n}$ — разложение на простые множители, то

$$\textbf{а)}\ \varphi(m) = \varphi(p_1^{k_1})\varphi(p_2^{k_2}) \cdots \varphi(p_n^{k_n})\ ; \qquad \textbf{б)}\ \varphi(m) = m \cdot \left(1 - \frac{1}{p_1}\right) \cdot \dots \cdot \left(1 - \frac{1}{p_n}\right)\ .$$

А4-2. Найдите все m такие, что $\varphi(m) = 10$.

А4-3. Выясните, чему равно произведение всех обратимых элементов кольца $\mathbb{Z}/n\mathbb{Z}$ и докажите *теорему Эйлера*: если класс вычетов $a \mod n$ обратим, то $a^{\varphi(m)} \equiv 1(\mod m)$.

Функция Мёбиуса. Пусть число $m \in \mathbb{Z}$ разложено на простые множители:

$$m = p_1^{k_1} \cdot \dots \cdot p_n^{k_n}\ .$$

Значение *функции Мёбиуса* $\mu(m)$ на числе m по определению равно 0, если хоть один из показателей $k_i \geqslant 2$ (т. е. если m делится на ненулевой квадрат), и равно $(-1)^n$, если все показатели $k_1, k_2, \dots, k_n$ равны 1. В частности, при $m = 0$ имеем $\mu(1) \stackrel{\text{def}}{=} 1$.

А4-4. Убедитесь, что $\mu(m)$ является мультипликативным характером, и докажите тождество $\sum\limits_{d|n} \mu(d) = \begin{cases} 1\ , & \text{при} \quad n = 1 \\ 0\ , & \text{при} \quad n > 1 \end{cases}$.

А4-5. *Обращение Мёбиуса.* Пусть для функции $g(n)$ известны значения всех сумм $\sum\limits_{d|n} g(d) = \sigma(n)$. Докажите, что тогда функцию $g(n)$ можно восстановить из функции $\sigma(n)$ по формуле $g(n) = \sum\limits_{d|n} \mu(\frac{n}{d})\sigma(d)$;

А4-6. Подберите $f(n)$, для которой $\sum\limits_{d|n} f(d) = \ln(n)$.

А4-7. Докажите, что $\sum\limits_{d|m} \varphi(d) = m$.

Круговые многочлены. Комплексное число $\zeta \in \mathbb{C}$ называется *первообразным корнем n-той степени*, если все комплексные решения уравнеия $z^n = 1$ являются степенями ζ. Многочлен $f_n(x) \stackrel{\text{def}}{=} \prod\limits_{\zeta}(x - \zeta) \in \mathbb{C}[x]$, где ζ пробегает все различные первообразные корни степени n, называется *n-тым круговым многочленом.*

А4-8. Докажите, что ζ тогда и только тогда является первообразным корнем n-той степени, когда будучи корнем уравнения $z^n = 1$, ζ не будет удовлетворять ни одному из уравнений $z^k = 1$ с $k < n$ (в частности, первообразные корни n-той степени всегда имеются).

---

[1]функция $\mathbb{Z} \xrightarrow{f} \mathbb{C}$ называется *мультипликативным характером*, если $f(mn) = f(m)f(n)$ всякий раз, когда *НОД* $(m, n) = 1$

A4-9. Докажите, что $x^n - 1 = \prod\limits_{d|n} f_d(x)$ и используя подходящую модификацию обращения Мёбиуса, докажите, что $f_n(x) = \prod\limits_{d|n} (x^{\frac{n}{d}} - 1)^{\mu(d)}$.

A4-10. Докажите, что $\forall\, n \in \mathbb{N}$ n-тый круговой многочлен f_n является неприводимым над $\mathbb{Z}$ многочленом степени $\varphi(n)$ с целыми коэффициентами.

A4-11. Пусть $p \in \mathbb{N}$ – простое. Проверьте следующие свойства круговых многочленов:

а) $f_{2n}(x) = f_n(-x)$, если n нечётно **б)** $f_p(x) = x^{p-1} + \cdots + x + 1$

в) $f_{p^k}(x) = f_p\left(x^{p^{k-1}}\right)$ **г)** $f_{pm}(x) = \dfrac{f_m(x^p)}{f_m(x)}$, если $p \not| m$

A4-12. Докажите, что если $m = p_1^{k_1} \cdot \cdots \cdot p_n^{k_n}$ (p_i — различные простые числа), то

$$f_m(x) = f_{p_1 p_2 \cdots p_n}\left(x^{p_1^{k_1-1} \cdots p_n^{k_n-1}}\right) .$$

Первообразные корни в кольце вычетов. Пусть a – обратимый элемент кольца $\mathbb{Z}/n\mathbb{Z}$. Назовём *порядком* вычета a наименьшее натуральное число k такое, что $a^k = 1$. Элемент a называется *первообразным корнем по модулю n*, если все прочие обратимые вычеты являются его степенями.

A4-13. Докажите, что если порядки k_i вычетов a_i попарно взаимно просты, то порядок вычета $a = a_1 \cdot \cdots \cdot a_n$ равен $k = k_1 \cdot \cdots \cdot k_n$.

A4-14. Докажите, что если существуют вычеты порядков k и l, то существует вычет порядка $HOK\,(k, l)$ (наименьшее общее кратное k и l).

A4-15. Докажите, что для существования первообразного корня необходимо и достаточно существование обратимого вычета порядка $\varphi(n)$.

A4-16. Докажите, что первообразный корень по любому простому модулю всегда существует.

A4-17*. Пусть $p > 2$ — простое и ϱ — первообразный корень по модулю p. Докажите, что существует $\vartheta \in \mathbb{N}$, такое что $(\varrho + p\vartheta)^{p-1} \equiv 1 \mod p$, но $(\varrho + p\vartheta)^{p-1} \not\equiv 1 \mod p^2$, и что в этом случае класс $\varrho + p\vartheta$ будет первообразным корнем по модулю p^k для любого $k \in \mathbb{N}$.

A4-18*. Докажите, что для любого простого p существует первообразный корень по модулю $2 \cdot p^k$.

A4-19. Существует ли первообразный корень по модулю 21?

Квадратичная взаимность. Пусть p – простое число. Сопоставим каждому $n \in \mathbb{Z}$ *символ Лежандра - Якоби* $\left(\dfrac{n}{p}\right) \in \{-1\,, 0\,, 1\,\}$, значение которого равно нулю, если n делится на p, единице – если n является ненулевым квадратом по $\mod p$, и -1 — в остальных случаях.

A4-20. Докажите, что $\left(\dfrac{n}{p}\right)$ — мультипликативный характер и что $\sum\limits_{i=1}^{p-1} \left(\dfrac{i}{p}\right) = 0$.

A4-21*. Докажите, что знак $\left(\dfrac{m}{p}\right)$ совпадает со знаком произведения $\prod\limits_{j=1}^{(p-1)/2} \dfrac{\sin\left(m \cdot 2\pi j / p\right)}{\sin\left(2\pi j / p\right)}$.

Указание: воспользуйтесь леммой Гаусса из листка «Сравнения и вычеты».

A4-22*. Докажите *квадратичный закон взаимности Гаусса*: для любых простых чисел p, q

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} .$$

Указание: воспользуйтесь предыдущей задачей и разложите все перемножаемые дроби на множители по формулам из листка «Комплексные числа».

A4-23. Найдите $\left(\dfrac{43}{109}\right)$.