О п р е д е л е н и е. Для любого целого положительного n *функция Эйлера* $\varphi(n)$ определяется как число неотрицательных целых b, меньших n и взаимно простых с n:

$$\varphi(n) \underset{\text{def}}{=} |\{0 \leqslant b < n \mid \text{НОД}\ (b, n) = 1\}|.$$

Легко проверить, что $\varphi(1) = 1$ и что $\varphi(p) = p - 1$ для любого простого p. Можно убедиться также, что для любого простого p

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^\alpha \left(1 - \frac{1}{p}\right).$$

Для этого достаточно заметить, что числа от 0 до $p^{\alpha}-1$, которые *не* взаимно просты с p^{α}, — это в точности те числа, которые делятся на p, а их количество равно $p^{\alpha-1}$.

Предложение (Китайская теорема об остатках). *Пусть требуется решить систему сравнений по различным модулям:*

$$\begin{aligned} x &\equiv a_1 \pmod{m_1}, \\ x &\equiv a_2 \pmod{m_2}, \\ &\cdots\cdots \\ x &\equiv a_r \pmod{m_r}, \end{aligned}$$

причем любые два модуля взаимно просты: НОД $(m_i, m_j) = 1$ *для* $i \neq j$. *Тогда эта система разрешима и любые два решения сравнимы по модулю* $M = m_1 m_2 \cdots m_r$.

Доказательство. Сначала докажем единственность по модулю M (последнее утверждение теоремы). Пусть x' и x'' — два решения системы. Положим $x = x' - x''$. Тогда x сравним с нулем по любому модулю m_i, а значит, и по модулю M (по пятому свойству сравнений). Теперь покажем, как найти решение x.

Обозначим через $M_i = M/m_i$ произведение всех модулей, кроме i-го. Очевидно, что НОД $(m_i, M_i) = 1$ и, следовательно, существует такое целое N_i, что $M_i N_i \equiv 1 \pmod{m_i}$ (число N_i может быть найдено, например, по алгоритму Евклида). Положим теперь $x = \sum_i a_i M_i N_i$. Тогда для каждого i все слагаемые в этой сумме, за исключением i-го, делятся на m_i, так как $m_i | M_j$ для всех $i \neq j$. Таким образом, для каждого i имеем $x \equiv a_i M_i N_i \equiv a_i \pmod{m_i}$, что и требовалось доказать.

Следствие. *Функция Эйлера обладает свойством «мультипликативности», т. е.* $\varphi(mn) = \varphi(m)\varphi(n)$, *если* НОД $(m, n) = 1$.

Доказательство следствия. Для доказательства необходимо подсчитать количество целых чисел между нулем и $mn-1$, не имеющих общих делителей с mn. Для каждого j из этого множества обозначим через j_1 наименьший неотрицательный вычет по модулю m (т.е. $0 \leqslant j_1 < m$ и $j \equiv j_1 \pmod m$) и через j_2 наименьший неотрицательный вычет по модулю n (т.е. $0 \leqslant j_2 < n$ и $j \equiv j_2 \pmod n$). Из китайской теоремы об остатках следует, что каждой паре j_1, j_2 соответствует одно и только одно число j в промежутке от 0 до $mn-1$, для которого $j \equiv j_1 \pmod m$ и $j \equiv j_2 \pmod n$. Заметим, что число j не имеет общих делителей с mn тогда и только тогда, когда оно не имеет общих делителей с m (это эквивалентно взаимной простоте j_1 и m) и не имеет общих делителей с n (что эквивалентно взаимной

простоте j_2 и n). Таким образом, числа j, взаимно простые с mn, находятся во взаимно однозначном соответствии с парами j_1, j_2, для которых $0 \leqslant j_1 < m$, НОД $(j_1, m) = 1$, $0 \leqslant j_2 < n$, НОД $(j_2, n) = 1$. Число возможных значений для j_1 равно $\varphi(m)$, а для j_2 равно $\varphi(n)$. Итак, число пар равно $\varphi(m)\varphi(n)$. Следствие доказано.

Поскольку каждое число n может быть представлено в виде произведения степеней различных простых чисел и уже установлена формула $\varphi(p^\alpha) = p^\alpha(1 - p^{-1})$, следствие означает, что при $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$

$$\varphi(n) = p_1^{\alpha_1}\left(1 - \frac{1}{p_1}\right) p_2^{\alpha_2}\left(1 - \frac{1}{p_2}\right) \cdots p_r^{\alpha_r}\left(1 - \frac{1}{p_r}\right)$$

$$= n \prod_{p|n}\left(1 - \frac{1}{p}\right).$$

Найти наименьшее неотрицательное решение каждой из следующих систем сравнений:

а)
$$\begin{aligned} x &\equiv 2 \pmod 3 \\ x &\equiv 3 \pmod 5 \\ x &\equiv 4 \pmod{11} \\ x &\equiv 5 \pmod{16} \end{aligned}$$

Найти наименьшее неотрицательное решение каждой из следующих систем сравнений:

б)
$$\begin{cases} x \equiv 12 \pmod{31} \\ x \equiv 87 \pmod{127} \\ x \equiv 91 \pmod{255} \end{cases}$$

Найти наименьшее неотрицательное решение каждой из следующих систем сравнений:

в)
$$\begin{cases} 19x \equiv 103 \pmod{900} \\ 10x \equiv 511 \pmod{841} \end{cases}$$

Перехвачено сообщение «S GNLIKD?KOZQLLIOMKUL.VY» (пробел после S является частью сообщения). Предположим, что использовано линейное шифрующее преобразование $C = AP$ в 30-буквенном алфавите, в котором A–Z имеют числовые эквиваленты 0–25, пробел = 26, . = 27, , = 28, ? = 29. Известно также, что последние шесть букв открытого текста — подпись KARLA и точка. Найти дешифрующую матрицу A^{-1} и весь открытый текст.