ДЗ 10
(криптография и теория чисел)

Владимир Латыпов
donrumata03@gmail.com

Содержание

4 ...

$$\varphi(n) = (p-1)(q-1) = pq - q - p + 1$$
$$n = pq$$
$$n - \varphi(n) = p + q - 1$$
$$p = \frac{n}{q}$$
$$\frac{n}{q} + q - 1 = n - \varphi(n)$$
$$\frac{n}{q} + q - 1 - (n - \varphi(n)) = 0$$
$$n + q^2 - q(1 - (n - \varphi(n))) = 0$$
$$a = 1, b = -(1 - (n - \varphi(n))), c = n$$
$$D = b^2 - 4ac$$
$$q = \frac{-b + -\sqrt{D}}{2}a$$
$$q = \left((1 - (n - \varphi(n))) + -\sqrt{(1 - (n - \varphi(n)))^2 - 4n}\right) \mid 2$$
$$p = \frac{N}{q}$$

18 gcd декомпозиция таблицы

Условие 18.1 Дана таблица $d[i, j]$. Построить массивы a и b такие, что $\operatorname{gcd}(a_i, b_j) = d[i, j]$.

Заметим, что

$$\begin{cases} \forall j : a_i \vdots d[i, j] \Rightarrow a_i = c \operatorname*{lcm}_{k \in [1, n]} d[i, k] \\ \forall i : b_j \vdots d[i, j] \Rightarrow b_j = c \operatorname*{lcm}_{k \in [1, n]} d[k, j] \end{cases}$$

Возьмём $c := 1$ везде. Пройдёмся по таблице и проверим, что $\operatorname{gcd}(a_i, b_j) = d[i, j]$.

- Всегда верно, что $\operatorname{gcd}(a_i, b_j) \geq d[i, j]$, так как a_i и b_j оба делятся на $d[i, j]$.
- Если нашлось $d[i, j]$, для которого $\operatorname{gcd}(a_i, b_j) > d[i, j]$, задача не имеет решения, так как это неравенство останется для любого выбора c-шек.