Поиск обратного в $\mathbb{Z}_m$ с помощью расширенного алгоритма Евклида и теоремы Эйлера

Лесников Юрий, ceagest

1 Обратный элемент

Определение 1.1. *Обратным по модулю m к целому числу a будем называть такое целое число b, что $ab \equiv 1 \pmod m$. Обозначение: $b = a^{-1}$.*

2 Поиск обратного в $\mathbb{Z}_m$

Теорема 2.1. *Пусть $n, m, d \in \mathbb{N}$. Тогда $\exists a, b \in \mathbb{Z} : an + bm = d \iff d \vdots \gcd(m, n)$*

Доказательство. Пусть $k = \gcd(n, m)$, $n = n_1 k, m = m_1 k$, где $n_1, m_1 \in \mathbb{N}, \gcd(n_1, m_1) = 1$. Тогда $k(an_1 + bm_1) = d$. Отсюда легко видеть, что необходимое условие разрешимости в целых числах – это $d \vdots k$. Покажем, что этого достаточно. Пусть $d = d_1 k$, где $d_1 \in \mathbb{N}$. Тогда $an_1 + bm_1 = d_1$ и $\gcd(n_1, m_1) = 1$. По теореме о линейном представлении НОД (тождество Безу) получаем, что $\exists x, y \in \mathbb{Z} : n_1 x + m_1 y = 1$. Домножив это равенство на d_1 и положив $a = d_1 x, b = d_1 y$, получим требуемое. □

2.1 Поиск обратного в $\mathbb{Z}_m$ с помощью расширенного алгоритма Евклида

Пусть $a \in \mathbb{Z}_m : \gcd(a, m) = 1$. С помощью расширенного алгоритма Евклида находим $x, y \in \mathbb{Z}$ такие, что $ax + my = \gcd(a, m) = 1$. Тогда $1 \equiv ax + my \equiv ax \pmod m$. Отсюда по определению x – обратный к a по модулю m.

2.2 Поиск обратного в $\mathbb{Z}_m$ с помощью теоремы Эйлера

Пусть $a \in \mathbb{Z}_m : \gcd(a, m) = 1$. Тогда из теоремы Эйлера получим:

$$a^{\varphi(m)} \equiv 1 \pmod m \implies a^{\varphi(m)} \cdot a^{-1} \equiv a^{-1} \pmod m \iff a^{\varphi(m)-1} \equiv a^{-1} \pmod m$$