Теорема (решение линейных диофантовых уравнений).

Обозначение: (a, b) - наибольший общий делитель a и b.

Уравнение $ax + by = c$ разрешимо в целых числах x, y тогда и только тогда, когда $(a, b)|c$. В случае разрешимости множество решений бесконечно. Все они имеют вид

$$\begin{cases} x = x_0 + \dfrac{b}{(a,b)}\,t, \\ y = y_0 - \dfrac{a}{(a,b)}\,t, \end{cases}$$

где пара чисел x_0, y_0 - какое-либо фиксированное решение, а t - произвольное целое число.

Как найти (x_0, y_0)? Существует три способа.

1. Угадать
2. Воспользоваться алгоритмом Евклида
3. Воспользоваться цепными дробями

Способ 2. Основан на следующей лемме

Если a, b - целые числа, то найдутся такие целые числа u и v, что $au + bv = (a, b)$

Тогда $x_0 = \frac{u \cdot c}{(a,b)}, \quad y_0 = \frac{v \cdot c}{(a,b)}$

Рассмотрим этот способ на примере $a = 3990, b = 1221$

Пользуясь алгоритмом Евклида, находим

$$3990 = 1221 \cdot 3 + 327$$
$$1221 = 327 \cdot 3 + 240$$
$$327 = 240 \cdot 1 + 87$$
$$240 = 87 \cdot 2 + 66$$
$$87 = 66 \cdot 1 + 21$$
$$66 = 21 \cdot 3 + 3$$
$$21 = 3 \cdot 7$$

Следовательно, $(3990, 1221) = 3$. Далее будем выражать остатки «снизу вверх», начиная с 6 строчки.

$$(3990, 1221) = 66 - 21 \cdot 3 = 66 - (87 - 66 \cdot 1) \cdot 3 = 66 \cdot 4 - 87 \cdot 3 =$$
$$= (240 - 87 \cdot 2) \cdot 4 - 87 \cdot 3 = 240 \cdot 4 - 87 \cdot 11 = 240 \cdot 4 - (327 - 240 \cdot 1) \cdot 11 =$$
$$= 240 \cdot 15 - 327 \cdot 11 = (1221 - 327 \cdot 3) \cdot 15 - 327 \cdot 11 = 1221 \cdot 15 - 327 \cdot 56 =$$
$$= 1221 \cdot 15 - (3990 - 1221 \cdot 3) \cdot 56 = 1221 \cdot 183 - 3990 \cdot 56$$

Таким образом, $u = -56, v = 183$.

Способ 3. Воспользуемся следующим свойством цепных дробей.

Пусть $\frac{P_{k-1}}{Q_{k-1}}, \frac{P_k}{Q_k}$ - две последовательные подходящие дроби к числу $\alpha \in \mathbb{R}$. Тогда $P_k Q_{k-1} - P_{k-1} Q_k = (-1)^{k+1}$.

Алгоритм.

1) Рассмотрим дробь $\frac{a}{b}$. Если она сократима, то сократить. Положим $a' = \frac{a}{(a,b)}, b' = \frac{b}{(a,b)}$.

2) Разложим число $\frac{a'}{b'}$ в цепную дробь. Это конечная цепная дробь, следовательно для какого-то целого n будет выполнено $a' = P_n, \quad b' = Q_n$. Используя написанное выше свойство мы находим такие u, v, что $a'u + b'v = 1$ следующим образом:

а) если n – нечетное, то $u' = Q_{n-1}, v' = -P_{n-1}$
б) если n – четное, то $u' = -Q_{n-1}, v' = P_{n-1}$

3) Очевидно, что $au + bv = (a, b)$. Аналогично, Тогда $x_0 = \frac{u \cdot c}{(a,b)}, \quad y_0 = \frac{v \cdot c}{(a,b)}$.

Рассмотрим тот же пример.
Сократим $\frac{3990}{1221} = \frac{1330}{407}$. Разложим в цепную дробь $\frac{1330}{407} = [3; 3, 1, 2, 1, 3, 7]$.

Контрольный вопрос. А почему разложение у этих двух дробей совпадает? И почему его можно взять из алгоритма Евклида способа 2?

n	-1	0	1	2	3	4	5	6
a_n		3	3	1	2	1	3	7
P_n	1	3	10	13	36	49	183	1330
Q_n	0	1	3	4	11	15	56	407

Так как $n = 6$, то $u = -56, v = 183$.

Решим теперь уравнение $3990x + 1221y = 12$.
Используя полученные результаты, получаем $x_0 = -56 \cdot 4 = -224, y_0 = 183 \cdot 4 = 732$.

$$\begin{cases} x = -224 + 407t, \\ y = 732 - 1330t \end{cases}$$

Теорема (решение сравнений первой степени).
Обозначение: (a, b) - наибольший общий делитель a и b.

Сравнение $ax \equiv c \ (mod\ b)$ разрешимо если и только если $(a, b)|c$. В случае разрешимости каждое решение x сравнимо с одним из

$$x_k = x_0 + \frac{b}{(a, b)}k$$

где x_0 - какое-либо фиксированное решение, а $k = 1, 2, \dots, (a, b)$.

Решим сравнение $3990x \equiv 12 \ (mod\ 1221)$.
Тогда $x_k = -224 + 407k, k = 1, 2, 3$.
Итого решения: $x \equiv 183 \ (mod\ 1221), x \equiv 590 (mod\ 1221), x \equiv 997 \ (mod\ 1221)$

Китайская теорема об остатках.

Если $m_1, m_2, \dots, m_k$ попарно взаимно просты, то система уравнений

$$\begin{cases} x \equiv a_1 (mod\ m_1) \\ x \equiv a_2 (mod\ m_2) \\ \cdots \\ x \equiv a_k (mod\ m_k) \end{cases}$$

разрешима. Определим целые числа M, M_i, b_i условиями

$$M = m_1 m_2 \dots m_k, \quad M_i = \frac{M}{m_i}, \quad M_i b_i \equiv a_i (mod\ m_i), \quad 1 \le i \le k.$$

Тогда решениями являются все такие x, что

$$x \equiv M_1 b_1 + \cdots + M_k b_k (mod\ M).$$

Решим систему сравнений

$$\begin{cases} x \equiv 3\ (mod\ 7) \\ x \equiv 2\ (mod\ 11) \\ x \equiv 1\ (mod\ 13) \end{cases}$$

Заметим, что 7, 11, 13 взаимно просты. Тогда $M = 7 \cdot 11 \cdot 13 = 1001, M_1 = 11 \cdot 13 = 143,$ $M_2 = 7 \cdot 13 = 91,\ M_3 = 7 \cdot 11 = 77.$

Решим вспомогательные сравнения (можно найти любое решение)

$$\begin{cases} 143b_1 \equiv 3\ (mod\ 7) \\ 91b_2 \equiv 2\ (mod\ 11) \\ 77b_3 \equiv 1\ (mod\ 13) \end{cases}$$

Тогда $b_1 = 1, b_2 = -3, b_3 = -1.$

Ответ: $x \equiv 143 \cdot 1 + 91 \cdot (-3) + 77 \cdot (-1) \equiv -207\ (mod\ 1001)$