Решение сравнений первой степени и их систем. Китайская теорема об остатках

1. Простые числа и основная теорема арифметики

Определение. Число $p \in \mathbb{N}$, $p \neq 1$, называется простым, если p имеет в точности два положительных делителя: 1 и p. Остальные натуральные числа (кроме 1) принято называть составными. Число 1 - на особом положении, по договору, оно ни простое, ни составное.

Теорема 1. Наименьший делитель любого числа $a \in \mathbb{N}$, отличный от 1, есть число простое.

Доказательство. Пусть $c \mid a$, $c \neq 1$ и c - наименьшее с этим свойством. Если существует c_1 такое, что $c_1 \mid c$, то $c_1 \leq c$ и $c_1 \mid a$, следовательно, $c_1 = c$ или $c_1 = 1$. ■

Теорема 2. Наименьший отличный от 1 делитель составного числа $a \in \mathbb{N}$ не превосходит $\sqrt{a}$.

Доказательство. $c \mid a$, $c \neq 1$, c - наименьший, следовательно, $a = ca_1$, $a_1 \mid a$, $a_1 \geq c$, значит, $aa_1 \geq c^2 a_1$, $a \geq c^2$ и $c \leq \sqrt{a}$. ■

Теорема (Евклид). Простых чисел бесконечно много.

Доказательство. От противного. Пусть $p_1, p_2, \ldots, p_n$ - все простые, какие только есть. Рассмотрим число $a = p_1, p_2, \ldots, p_n + 1$. Его наименьший отличный от 1 делитель c, будучи простым, не может совпадать ни с одним из $p_1, p_2, \ldots, p_n$, так как иначе $c \mid 1$. ■

Для составления таблицы простых чисел древний грек Эратосфен придумал процедуру, которая получила название «решето Эратосфена»:

2, 3, ~~4~~, 5, ~~6~~, 7, ~~8~~, ~~9~~, ~~10~~, 11, ~~12~~, 13, ~~14~~, ~~15~~, ~~16~~, 17, …

Идем по натуральному ряду слева направо. Подчеркиваем первое неподчеркнутое и невычеркнутое число, а из дальнейшего ряда вычеркиваем кратные только что подчеркнутому. И так много раз. Легко понять, что подчеркнутые числа – простые. Если вспомнить теорему 2, то становится понятно, что когда вычеркнуты все кратные простых, меньших p, то оставшиеся невычеркнутые, меньшие p^2 - простые. Это значит, что составление таблицы всех простых чисел меньших N закончено сразу, как только вычеркнуты все кратные простых, меньших $\sqrt{a}$.

Теорема 3. Всякое целое число, отличное от -1, 0, и 1, единственным образом (с точностью до порядка сомножителей) разложимо в произведение простых чисел.

Доказательство. Будем доказывать утверждение теоремы только для натуральных чисел.

Пусть $a>1$, p_1 - его наименьший простой делитель. Значит, $a=p_1a_1$. Если, далее, $a_1>1$, то пусть p_2 - его наименьший простой делитель и $a_1=p_2a_2$, т.е. $a=p_1p_2a_2$, и так далее, пока a_n не станет равным единице. Это обязательно произойдет, так как $a>a_1>a_2\ldots$. Имеем, таким образом, $a=p_1p_2\ldots p_n$, и возможность разложения доказана.

Теорема 3. Всякое целое число, отличное от -1, 0, и 1, единственным образом (с точностью до порядка сомножителей) разложимо в произведение простых чисел.

Покажем единственность. Пусть $a = q_1 q_2 ... q_s$ - другое разложение, т.е. $p_1 p_2 ... p_n = q_1 q_2 ... q_s$. В последнем равенстве правая часть делится на q_1, следовательно, левая часть делится на q_1. Покажем, что если произведение $p_1 p_2 ... p_n$ делится на q_1, то один из сомножителей p_k обязан делиться на q_1.

Действительно, если $q_1 \mid p_1$, то все доказано. Пусть q_1 не делит p_1. Так как q_1 - простое число, то $(q_1, p_1) = 1$. Значит, найдутся такие $u, v \in$, что $up_1 + vq_1 = 1$. Умножим последнее равенство на $p_2 ... p_n$, получим: $p_2 ... p_n = p_1 (p_2 ... p_n) u + q_1 (p_2 ... p_n) v$. Оба слагаемых справа делятся на q_1, следовательно, $p_2 ... p_n$ делится на q_1. И так далее, по индукции.

Теперь, пусть, например, $q_1 \mid p_1$. Значит, $q_1 = p_1$, так как p_1 - простое. Из равенства $p_1 p_2 ... p_n = q_1 q_2 ... q_s$ сокращением получим равенство $p_2 ... p_n = q_2 ... q_s$. Снова рассуждая по индукции, видим, что $n = s$, и каждый сомножитель левой части равенства $p_1 p_2 ... p_n = q_1 q_2 ... q_n$ обязательно присутствует в правой и наоборот. ■

Следствие 1. Всякое рациональное число однозначно представимо в виде $p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$, где $\alpha_1, \alpha_2, \ldots, \alpha_k \in \mathbb{Z}$.

Следствие 2. Если $a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_n^{\alpha_n}$, $b = p_1^{\beta_1} p_2^{\beta_2} \ldots p_n^{\beta_n}$ - целые числа, то наибольший общий делитель a и b равен $p_1^{\gamma_1} p_2^{\gamma_2} \ldots p_n^{\gamma_n}$, а наименьшее общее кратное a и b равно $p_1^{\delta_1} p_2^{\delta_2} \ldots p_n^{\delta_n}$, где $\gamma_i = \min\{\alpha_i, \beta_i\}$, а $\delta_i = \max\{\alpha_i, \beta_i\}$.

2. Теория сравнений

Определение. Пусть $a, b \in \mathbb{Z}$, $m \in \mathbb{Z}$. Говорят, что число a сравнимо с b по модулю m, если a и b при делении на m дают одинаковые остатки. Запись выглядит следующим образом: $a \equiv b \pmod{m}$.

Ясно, что число a сравнимо с b по модулю m тогда и только тогда, когда $a - b$ делится на m нацело. Очевидно, это бывает тогда и только тогда, когда найдется такое целое число t, что $a = b + mt$.

Свойство 1. Сравнения по одинаковому модулю можно почленно складывать.

Доказательство. Пусть $a_1 \equiv b_1 \pmod{m}$, $a_2 \equiv b_2 \pmod{m}$. Это означает, что $a_1 = b_1 + mt_1$, $a_2 = b_2 + mt_2$ После сложения последних двух равенств получим $a_1 + a_2 = b_1 + b_2 + m(t_1 + t_2)$, что означает $a_1 + a_2 \equiv b_1 + b_2 \pmod{m}$.■

Свойство 2. Слагаемое, стоящее в какой-либо части сравнения, можно переносить в другую часть, изменив его знак на обратный.

Доказательство.

$$\begin{cases} a + b \equiv c \pmod{m} \\ -b \equiv -b \pmod{m} \end{cases} +$$

$$\overline{a \equiv c - b \pmod{m}}$$

■

Свойство 3. К любой части сравнения можно прибавить любое число, кратное модулю.

Доказательство.

$$\begin{cases} a \equiv b(\mathrm{mod}\, m) \\ mk \equiv 0(\mathrm{mod}\, m) \end{cases} +$$

$$a + mk \equiv b(\mathrm{mod}\, m)$$

■

Свойство 4. Сравнения по одинаковому модулю можно почленно перемножать.

Свойство 5. Обе части сравнения можно возвести в одну и ту же степень.

$$\begin{cases} a_1 \equiv b_1 \pmod{m} \Leftrightarrow a_1 = b_1 + mt_1 \\ a_2 \equiv b_2 \pmod{m} \Leftrightarrow a_2 = b_2 + mt_2 \end{cases} \times$$

$$a_1 a_2 = b_1 b_2 + m(b_1 t_2 + b_2 t_1 + m t_1 t_2) \Rightarrow a_1 a_2 \equiv b_1 b_2 \pmod{m}.$$

Свойство 6. Если $a_0 \equiv b_0 \pmod m$, $a_1 \equiv b_1 \pmod m$, …, $a_n \equiv b_n \pmod m$, $x \equiv y \pmod m$, то $a_0 x^n + a_1 x^{n-1} + \ldots + a_n \equiv b_0 y^n + b_1 y^{n-1} + \ldots + b_n \pmod m$.

Свойство 7. Обе части сравнения можно разделить на их общий делитель, взаимно простой с модулем.

Доказательство. Пусть $a \equiv b \pmod m$, $a = a_1 d$, $b = b_1 d$. Тогда $(a_1 - b_1)d$ делится на m. Поскольку d и m взаимно просты, то на m делится именно $(a_1 - b_1)$, что означает $a_1 \equiv b_1 \pmod m$. ■

Свойство 8. Обе части сравнения и его модуль можно умножить на одно и то же целое число или разделить на их общий делитель.

Доказательство.

$$a \equiv b \left(\operatorname{mod} m\right) \Leftrightarrow a = b + mt \Leftrightarrow ak = bk + mkt \Leftrightarrow ak \equiv bk \left(\operatorname{mod} mk\right). \blacksquare$$

Свойство 9. Если сравнение $a \equiv b$ имеет место по нескольким разным модулям, то оно имеет место и по модулю, равному наименьшему общему кратному этих модулей.

Доказательство. Пусть $a \equiv b \left(\operatorname{mod} m_1\right)$ и $a \equiv b \left(\operatorname{mod} m_2\right)$, $a - b$ делится на m_1 и на m_2, значит, $a - b$ делится на наименьшее общее кратное m_1 и на m_2.

Свойство 10. Если сравнение имеет место по модулю m, то оно имеет место и по модулю d, равному любому делителю числа m.

Доказательство, очевидно, следует из транзитивности отношения делимости: если $a \equiv b \pmod{m}$, $a-b$ делится на m, значит, $a-b$ делится на d, где $d \mid m$. ■

Свойство 11. Если одна часть сравнения и модуль делятся на некоторое число, то и другая часть сравнения должна делиться на то же число.

Доказательство.

$$a \equiv b \pmod{m} \Leftrightarrow a = b + mt \text{ . } \blacksquare$$

Пример. Доказать, что при любом натуральном n число $37^{n+2}+16^{n+1}+23^n$ делится на 7.

Решение. Очевидно, что $37\equiv 2\pmod 7$, $16\equiv 2\pmod 7$, $23\equiv 2\pmod 7$.

Возведем первое сравнение в степень $n+2$, второе – в степень $n+1$, третье – в степень n и сложим:

$$\begin{aligned} 37^{n+2} &\equiv 2^{n+2} \pmod 7, \\ 16^{n+1} &\equiv 2^{n+1} \pmod 7, \quad + \\ 23^{n} &\equiv 2^{n} \pmod 7, \\ \hline 37^{n+2}+16^{n+1}+23^{n} &\equiv 2^{n}\cdot 7 \pmod 7 \end{aligned}$$

т.е. $37^{n+2}+16^{n+1}+23^n$ делится на 7.

3. Вычеты. Полная и приведенная системы вычетов

Определение. Любое число из класса эквивалентности $\equiv_m$ будем называть вычетом по модулю m. Совокупность вычетов, взятых по одному из каждого класса эквивалентности $\equiv_m$, называется полной системой вычетов по модулю m (в полной системе вычетов, таким образом, всего m штук чисел). Непосредственно сами остатки при делении на m называются наименьшими неотрицательными вычетами и образуют полную систему вычетов по модулю m. Вычет ρ называется абсолютно наименьшим, если $|\rho|$ наименьший среди модулей вычетов данного класса.

Пример: Пусть $m = 5$. Тогда:

0, 1, 2, 3, 4 - наименьшие неотрицательные вычеты;

-2, -1, 0, 1, 2 - абсолютно наименьшие вычеты.

Обе приведенные совокупности чисел образуют полные системы вычетов по модулю 5.

Лемма 1. 1) Любые m штук попарно не сравнимых по модулю m чисел образуют полную систему вычетов по модулю m.

2) Если a и m взаимно просты, а x пробегает полную систему вычетов по модулю m, то значения линейной формы $ax+b$, где b - любое целое число, тоже пробегают полную систему вычетов по модулю m.

Доказательство. Утверждение 1) – очевидно. Докажем утверждение 2). Чисел $ax+b$ ровно m штук. Покажем, что они между собой не сравнимы по модулю m. Ну пусть для некоторых различных x_1 и x_2 из полной системы вычетов оказалось, что $ax_1+b \equiv ax_2+b \pmod{m}$. Тогда, по свойствам сравнений из предыдущего пункта, получаем:

$$ax_1 \equiv ax_2 \pmod{m}$$

$$x_1 \equiv x_2 \pmod{m}$$

– противоречие с тем, что x_1 и x_2 различны и взяты из полной системы вычетов. ■

Определение. Приведенной системой вычетов по модулю m называется совокупность всех вычетов из полной системы, взаимно простых с модулем m.

Приведенную систему обычно выбирают из наименьших неотрицательных вычетов. Ясно, что приведенная система вычетов по модулю m содержит $\varphi(m)$ штук вычетов, где $\varphi(m)$ – функция Эйлера – число чисел, меньших m и взаимно простых с m.

Пример. Пусть $m = 42$. Тогда приведенная система вычетов выглядит следующим образом:

$$1, 5, 11, 13, 17, 19, 23, 25, 29, 31, 37, 41.$$

Лемма 2. 1) Любые $\varphi(m)$ чисел, попарно не сравнимые по модулю m и взаимно простые с модулем, образуют приведенную систему вычетов по модулю m. 2) Если $(a,m)=1$ и x пробегает приведенную систему вычетов по модулю m, то ax так же пробегает приведенную систему вычетов по модулю m.

Доказательство. Утверждение 1) – очевидно. Докажем утверждение 2). Числа ax попарно несравнимы (это доказывается так же, как в лемме 1 этого пункта), их ровно $\varphi(m)$ штук. Ясно также, что все они взаимно просты с модулем, ибо $(a,m)=1,\ (x,m)=1\Rightarrow(ax,m)=1$. Значит, числа ax образуют приведенную систему вычетов. ■

Лемма 3. Пусть $m_1, m_2, \ldots, m_k$ - попарно взаимно просты и $m_1, m_2, \ldots, m_k = M_1 m_1 = M_2 m_2 = \ldots = M_k m_k$, где $M_j = m_1 \ldots m_{j-1} m_{j+1} \ldots m_k$.

1) Если $x_1, x_2, \ldots, x_k$ пробегают полные системы вычетов по модулям $m_1, m_2, \ldots, m_k$ соответственно, то значения линейной формы $M_1 m_1 + M_2 m_2 + \ldots + M_k m_k$ пробегают полную систему вычетов по модулю $m = m_1 m_2 \ldots m_k$.

2) Если $\xi_1, \xi_2, \ldots, \xi_k$ пробегают приведенные системы вычетов по модулям $m_1, m_2, \ldots, m_k$ соответственно, то значения линейной формы $M_1 \xi_1 + M_2 \xi_2 + \ldots + M_k \xi_k$ пробегают приведенную систему вычетов по модулю $m = m_1 m_2 \ldots m_k$.

Доказательство.

1) Форма $M_1 m_1 + M_2 m_2 + ... + M_k m_k$ принимает, очевидно, $m_1 m_2 ... m_k = m$ значений. Покажем, что эти значения попарно несравнимы. Пусть

$$M_1 x_1 + M_2 x_2 + ... + M_k x_k \equiv M_1 x_1^{\nabla} + M_2 x_2^{\nabla} + ... + M_k x_k^{\nabla} \left(\mathrm{mod}\, m\right).$$

Всякое M_j, отличное от M_s, кратно m_s. Убирая слева и справа в последнем сравнении слагаемые, кратные m_s, получим:

$$M_s x_s \equiv M_s x_s^{\nabla} \left(\mathrm{mod}\, m_s\right) \Rightarrow x_s \equiv x_s^{\nabla} \left(\mathrm{mod}\, m_s\right)$$

– противоречие с тем, что x_s пробегает полную систему вычетов по модулю m_s.

2) Форма $M_1 \xi_1 + M_2 \xi_2 + ... + M_k \xi_k$ принимает, очевидно, $\varphi\left(m_1\right)\varphi\left(m_2\right) \cdot ... \cdot \varphi\left(m_k\right) = \varphi\left(m_1 m_2 \cdot ... \cdot m_k\right) = \varphi\left(m\right)$ (функция Эйлера мультипликативна!) различных значений, которые между собой по модулю $m_1 m_2 ... m_k = m$ попарно несравнимы. Последнее легко доказывается рассуждениями, аналогичными рассуждениям, проведенным при доказательстве утверждения 1) этой леммы. Так как $\left(M_1 \xi_1 + M_2 \xi_2 + ... + M_k \xi_k, m_s\right) = \left(M_s \xi_s, m_s\right) = 1$ для каждого $1 \le s \le k$, то $\left(M_1 \xi_1 + M_2 \xi_2 + ... + M_k \xi_k, m_s\right) = 1$, следовательно множество значений формы $M_1 \xi_1 + M_2 \xi_2 + ... + M_k \xi_k$ образует приведенную систему вычетов по модулю m. ■

Лемма 4. Пусть $x_1, x_2, \ldots, x_k, x$ пробегают полные, а $\xi_1, \xi_2, \ldots, \xi_k, \xi$ - пробегают приведенные системы вычетов по модулям $m_1, m_2, \ldots, m_k$ и $m = m_1 m_2 \ldots m_k$ соответственно, где $(m_i, m_j) = 1$ при $i \neq j$. Тогда дроби $\left\{ \frac{x_1}{m_1} + \frac{x_1}{m_1} + \ldots + \frac{x_k}{m_k} \right\}$ совпадают с дробями $\left\{ \frac{x}{m} \right\}$, а дроби $\left\{ \frac{\xi_1}{m_1} + \frac{\xi_1}{m_1} + \ldots + \frac{\xi_k}{m_k} \right\}$ совпадают с дробями $\left\{ \frac{\xi}{m} \right\}$.

Доказательство. Доказательство обоих утверждений леммы 4 легко получается применением предыдущей леммы 3 после того, как вы приведете каждую сумму $\left\{\frac{x_1}{m_1}+\frac{x_1}{m_1}+\ldots+\frac{x_k}{m_k}\right\}$ и $\left\{\frac{\xi_1}{m_1}+\frac{\xi_1}{m_1}+\ldots+\frac{\xi_k}{m_k}\right\}$ к общему знаменателю:

$$\left\{\frac{x_1}{m_1}+\frac{x_2}{m_2}+\ldots+\frac{x_k}{m_k}\right\}=\left\{\frac{M_1x_1+M_2x_2+\ldots+M_kx_k}{m}\right\};$$

$$\left\{\frac{\xi_1}{m_1}+\frac{\xi_2}{m_2}+\ldots+\frac{\xi_k}{m_k}\right\}=\left\{\frac{M_1\xi_1+M_2\xi_2+\ldots+M_k\xi_k}{m}\right\},$$

где $M_j=m_1..m_{j-1}m_{j+1}...m_k$.

Если теперь принять во внимание, что дробные части чисел, получающихся при делении на модуль m любых двух чисел, сравнимых по модулю m, одинаковы (они равны r/m, где r – наименьший неотрицательный вычет из данного класса), то утверждения настоящей леммы становятся очевидными. ■

Замечание. Если от каждого класса вычетов по $\mathrm{mod}\, m$ взять по одному представителю, то мы получим *полную систему вычетов*.

1) 0, 1, 2, 3, 4 – полная система вычетов по $\mathrm{mod}\, 5$;
2) 5, 1, 2, -2, 4 – полная система вычетов по $\mathrm{mod}\, 5$;
3) 5, 1, 2, 4, 9, 5, 1, 2, 4 – не полная система вычетов по $\mathrm{mod}\, 5$;

Если в полной системе вычетов взяты все вычеты, взаимно простые с модулем, то система называется *приведенной*.

4. Решение сравнений первой степени

Определение. Сравнением первой степени называются уравнения вида $ax \equiv b \pmod{m}$.

Определение. Говорят, что $x \equiv x_0 \pmod{m}$ является решением сравнения $ax \equiv b \pmod{m}$, если верно $ax_0 \equiv b \pmod{m}$.

Теорема 1. Сравнение $ax \equiv 1 \pmod{m}$ разрешимо тогда и только тогда, когда НОД $(a,m) = 1$. Если сравнение разрешимо, то оно имеет единственное решение по модулю m.

Пример 1. Решить сравнение по определению:

а) $8x \equiv 11 (\mathrm{mod} 14)$;

б) $3x \equiv 5 (\mathrm{mod}\, 7)$.

Решение.

а) Задано $8x \equiv 11 (\mathrm{mod} 14)$, по определению сравнения получаем $14 \mid (8x - 11)$, но $(8x - 11)$ число нечетное при любом x. Значит, 14 не может делить $(8x - 11)$. Следовательно, сравнение не разрешимо.

б) Задано $3x \equiv 5 (\mathrm{mod}\, 7)$, по определению имеем: $7 \mid (3x - 5)$, т.е. $3x - 5 = 7k$, где k - целое число.

Выразим $x = \dfrac{5 + 7k}{3} = 1 + 2k + \dfrac{2 + k}{3}$, x - целое число, значит $(2 + k)$ должно делиться на 3. Возьмем в качестве $k = 1$, тогда $x = \dfrac{5 + 7}{3} = 4$. НОД(3, 7) = 1, то система имеет единственное решение по модулю 7.

Ответ. а) решения нет; б) $x \equiv 4 (\mathrm{mod}\, 7)$.

Пример 2. Решить сравнение, используя линейное представление НОД: $3x \equiv 5 \pmod 7$.

Решение. Задано $3x \equiv 5 \pmod 7$, НОД (3, 7) = 1, то система имеет единственное решение по модулю 7.

Найдем линейное представление НОД (3, 7) = 1.

$7 = 3 \cdot 2 + 1$;

$3 = 1 \cdot 3$.

Линейное представление НОД:

$1 = 7 + 3 \cdot (-2)$, тогда $3 \cdot (-2) \equiv 1 \pmod 7$.

Умножая на 5 обе части сравнения, получаем $3 \cdot ((-2) \cdot 5) \equiv 5 \pmod 7$, тогда $x \equiv (-2) \cdot 5 \pmod 7 \equiv -10 \pmod 7 \equiv 4 \pmod 7$.

Ответ. $x \equiv 4 \pmod 7$.

Пример 3. Решить сравнение $8x \equiv 12 \pmod{14}$ (случай не единственности решения).

Решение. $8x \equiv 12 \pmod{14}$. По свойствам сравнений разделим все три части сравнения на 2. Получим $4x \equiv 6 \pmod{7}$.

Упростим сравнение: $2x \equiv 3 \pmod{7}$. Решим любым способом (например, подбором): $x \equiv 5 \pmod{7}$. Так как НОД (2, 7) = 1, то решение единственно по $\mathrm{mod}\,7$. Теперь найдем решение по модулю 14: положим $x = 5 + 7t$, где t - целое число, тогда при $t = 0$, $x_1 \equiv 5 \pmod{14}$, при $t = 1$, $x_2 \equiv 5 + 7 \pmod{14} \equiv 12 \pmod{14}$.

При больших t получаем $5 + 7t > 14$, т.е. решения повторяются.

Ответ: $x_1 \equiv 5 \pmod{14}$, $x_2 \equiv 12 \pmod{14}$.

Пример 4. Решить уравнение $47x-111y=89$.

Решение. Условие уравнения можно переписать в следующем виде: $47x\equiv 89\left(\mathrm{mod}111\right)$.

Решим сравнение любым способом $x\equiv 94\left(\mathrm{mod}111\right)$, тогда $x=94+111t$. Подставим в уравнение:

$$94\cdot 47+111\cdot t\cdot 47-111\cdot y=89,$$

$$111\cdot t-111\cdot y=-111\cdot 39,$$

$$y=39+47\cdot t.$$

Ответ: $x=94+111t$, $y=39+47t$, где $t\in$.

5. Системы сравнений

Теорема (китайская теорема об остатках). Для натуральных чисел m_1 и m_2 таких что $\text{НОД}(m_1, m_2) = 1$ система сравнений

$$\begin{cases} x \equiv a \pmod{m_1} \\ x \equiv b \pmod{m_2} \end{cases}$$

разрешима и имеет единственное решение по модулю (m_1, m_2).

Доказательство. По условию $\text{НОД}(m_1, m_2) = 1$. Значит, существует линейное представление с целыми u и v такими, что $m_1 \cdot u + m_2 \cdot v = 1$. Рассмотрим $x = b \cdot m_1 \cdot u + a \cdot m_2 \cdot v$. Легко увидеть, что $x \equiv a \pmod{m_1}$ и $x \equiv b \pmod{m_2}$. Таким образом, решение системы существует. Пусть найдется другое решение $x = x_0$ этой системы: $x_0 \equiv a \pmod{m_1}$ и $x_0 \equiv b \pmod{m_2}$.

Тогда $x - x_0 \equiv 0 \pmod{m_1}$ и $x - x_0 \equiv 0 \pmod{m_2}$, следовательно, $m_1 \mid (x - x_0)$, $m_2 \mid (x - x_0)$. При условии $\text{НОД}(m_1, m_2) = 1$, $m_1 \cdot m_2 \mid (x - x_0)$, значит, $x_0 \equiv x \pmod{m_1 \cdot m_2}$. ■

Теорема. В условиях теоремы, решением системы является $x \equiv b \cdot m_1 \cdot u + a \cdot m_2 \cdot v \left(\mathrm{mod}\, m_1 \cdot m_2\right)$, где $m_1 \cdot u + m_2 \cdot v = 1$ - линейное представление $\mathrm{НОД}\left(m_1, m_2\right) = 1$.

Пример 5. Решить систему сравнений $\begin{cases} x \equiv 2 \pmod 5 \\ x \equiv 8 \pmod{11} \end{cases}$ любым способом.

Решение. Из первого сравнения системы получаем, что $x = 2 + 5t$, где $t \in \mathbb{Z}$.

Подставим во второе сравнение системы $2 + 5t \equiv 8 \pmod{11}$. Решим его: $5t \equiv 6 \pmod{11} \equiv -5 \pmod{11}$, $t \equiv 10 \pmod{11}$ или $t = 10 + 11k$, тогда $x = 2 + 5(10 + 11k) = 52 + 55k$.

Ответ: $x \equiv 52 \pmod{55}$.

Пример 6. Решить систему сравнений:

а) $\begin{cases} x \equiv 2 \pmod 5 \\ x \equiv 8 \pmod{11} \end{cases}$;

б) $\begin{cases} 4x \equiv 3 \pmod 5 \\ 3x \equiv 1 \pmod{10} \end{cases}$.

Решение.

а) Рассмотрим систему $\begin{cases} x \equiv 2 \pmod 5 \\ x \equiv 8 \pmod{11} \end{cases}$.

Модули обладают свойством НОД (5, 11) = 1, то решить систему можно по следствия китайской теоремы об остатках. Для этого найдем линейное представление НОД (5, 11):

$1 = 5 \cdot (-2) + 11 \cdot 1$.

Тогда по известным формулам имеем

$x = 2 \cdot (11 \cdot 1) + 8 \cdot (5 \cdot (-2))$, или

$x = 22 - 80 = -58$;

$x \equiv -58 \pmod{55} \equiv 52 \pmod{55}$.

б) $\begin{cases} 4x \equiv 3 \pmod 5 \\ 3x \equiv 1 \pmod{10} \end{cases}$.

Решим независимо каждое сравнение любым способом:

$$\begin{cases} x \equiv 12 \pmod{15} \\ x \equiv 7 \pmod{10} \end{cases}$$

Так как модули не взаимно простые, то решение находим по модулю НОК[10, 15] = 30. Из первого сравнения получаем: $x = 12 + 15k$, подставим во второе сравнение системы

$12 + 15k \equiv 7 \pmod{10}$; упростим

$15k \equiv -5 \pmod{10}$; $3k \equiv -1 \pmod 2$; $k \equiv 1 \pmod 2$, тогда $k = 1 + 2n$, где n - целое число; подставим k в формулу для x:

$$x = 12 + 15(1 + 2n) = 27 + 30n \equiv 27 \pmod{30}.$$

Ответ: а) $x \equiv 52 \pmod{55}$; $x \equiv 27 \pmod{30}$.