Раздел 8. Теория сравнений

Определения и простейшие свойства.

Определение 1. Пусть $a, b \in Z, m \in N$. Говорят, что число a сравнимо с b по модулю m, если a и b при делении на m дают одинаковые остатки. Запись этого факта выглядит так: $a \equiv b(\text{mod } m)$.

Определение 2. Два целых числа a и b называются сравнимыми по модулю m, если их разность делится нацело на m. $(a-b) \vdots m$

Определение 3. Два целых числа a и b называются сравнимыми по модулю m, если $a = b + mt$, где $t \in Z$.

Очевидно, что бинарное отношение сравнимости $\equiv_m$ (неважно, по какому модулю) есть отношение эквивалентности на множестве целых чисел.

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

Понять процесс собирания целых чисел в классы сравнимых между собой по модулю m (классы эквивалентности $\equiv_m$) поможет следующая картинка:

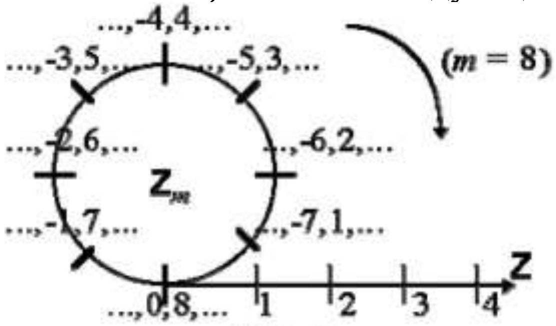

Рис. 6

На рисунке 6 изображен процесс наматывания цепочки целых чисел на колечко с m делениями, при этом на одно деление автоматически попадают сравнимые между собой числа. Кстати, эта картинка неплохо объясняет и термин "кольцо".

Перечислим, далее, свойства сравнений, похожие на свойства отношения равенства.

Свойство 1. Сравнения по одинаковому модулю можно почленно складывать.

Доказательство. Пусть $a_1 = b_1(\text{mod } m)$, $a_2 = b_2(\text{mod } m)$. 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 $a_1 + a_2 = b_1 + b_2(\text{mod } m)$.

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

Доказательство.

$$\begin{array}{l} \begin{cases} a + b \equiv c(\text{mod}\, m) \\ -b \equiv -b(\text{mod}\, m) \end{cases} + \\ \hline a \equiv c - b(\text{mod}\, m) \end{array}$$

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

Доказательство.

$$\begin{array}{l} \begin{cases} a \equiv b(\text{mod}\, m) \\ mk \equiv 0(\text{mod}\, m) \end{cases} + \\ \hline a + mk \equiv b(\text{mod}\, m) \end{array}$$

Свойство 4. Сравнения по одинаковому модулю можно почленно перемножать и, следовательно.

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

Доказательство.

$$\begin{array}{l}\left\{\begin{array}{l}a_1 \equiv b_1(\mathbf{mod}\,m) \Leftrightarrow a_1 = b_1 + mt_1\\ a_2 \equiv b_2(\mathbf{mod}\,m) \Leftrightarrow a_2 = b_2 + mt_2\end{array}\right. \times\\ \hline a_1a_2 = b_1b_2 + m(b_1t_2 + b_2t_1 + mt_1t_2) \Rightarrow a_1a_2 \equiv b_1b_2(\mathbf{mod}\,m).\end{array}$$

Как следствие из вышеперечисленных свойств, получаем

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

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

Доказательство. Пусть $a \equiv b($mod $m)$, $a = a_1 d$, $b = b_1 d$. Тогда $(a_1 - b_1)\cdot d$ делится на m.

Поскольку d и m взаимно просты, то на m делится именно $(a_1 - b_1)$, что означает $a_1 \equiv b_1($mod $m)$.

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

Доказательство. $a \equiv b($mod $m) \Leftrightarrow a = b + mt \Leftrightarrow ak = bk + mkt \Leftrightarrow ak \equiv bk($mod $mk)$.

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. Если $a \equiv b($mod $m_1)$ и $a \equiv b($mod $m_2)$, то a-b делится на m_1 и на m_2, значит a-b делится на наименьшее общее кратное m_1 и 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 $a \equiv b($mod $m)$, то a-b делится на m, значит a-b делится на d, где $d|m$.

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

Доказательство. $a \equiv b(mod\ m) \Leftrightarrow a=b+mt$.

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

Решение. Очевидно, что 37 ≡ 2(mod 7), 16 ≡ 2(mod 7), 23 ≡ 2(mod 7)

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

$$\begin{array}{l}37^{n+2} \equiv 2^{n+2}(\mathrm{mod}\,7),\\ 16^{n+1} \equiv 2^{n+1}(\mathrm{mod}\,7), \quad +\\ 23^{n} \equiv 2^{n}(\mathrm{mod}\,7),\\ \hline 37^{n+2} + 16^{n+1} + 23^{n} \equiv 2^{n}\cdot 7(\mathrm{mod}\,7)\end{array}$$

т.е. $37^{n+2} + 16^{n+1} + 23^n$ делится на 7. Как видите, ровным счетом ничего сложного в решении подобных школьных задач "повышенной трудности" нет.

С удовольствием заканчиваю настоящий пункт, чтобы устремиться к следующему, то есть устремиться из прошлого в будущее.

Полная и приведенная системы вычетов.

В предыдущем пункте было отмечено, что отношение $\equiv_m$ сравнимости по произвольному модулю m есть отношение эквивалентности на множестве целых чисел. Это отношение эквивалентности индуцирует разбиение множества целых чисел на классы эквивалентных между собой элементов, т.е. в один класс объединяются числа, дающие при делении на m одинаковые остатки. Число классов эквивалентности $\equiv_m$ (знатоки скажут – "индекс эквивалентности $\equiv_m$") в точности равно m.

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, конечно, 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 $ax_1 + b \equiv ax_2 + b (\mathrm{mod}\ m)$. 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.

Поскольку все числа из данного класса эквивалентности $\equiv_m$ получаются из одного числа данного класса прибавлением числа, кратного m, то все числа из данного класса имеют с модулем m один и тот же наибольший общий делитель. По некоторым соображениям, повышенный интерес представляют те вычеты, которые имеют с модулем m наибольший общий делитель, равный единице, т.е. вычеты, которые взаимно просты с модулем.

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 $\phi(m)$ штук вычетов, где $\phi(m)$– функция Эйлера – число чисел, меньших m и взаимно простых с m.

Функция Эйлера.

Функция Эйлера $\phi(a)$ есть количество чисел из ряда 0, 1, 2,..., a–1, взаимно простых с a.

Лемма. Пусть

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}.$$

Тогда:

1) $\varphi(a) = a\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_n}\right)$ (формула Эйлера);

2) $\varphi(a) = \left(p_1^{\alpha_1} - p_1^{\alpha_1-1}\right)\left(p_2^{\alpha_2} - p_2^{\alpha_2-1}\right)\cdots\left(p_n^{\alpha_n} - p_n^{\alpha_n-1}\right),$

в частности, $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$, $\varphi(p) = p-1$.

Пример. Пусть $m = 42$. Тогда приведенная система вычетов суть:

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

Лемма 2. 1) Любые $\phi(m)$ чисел, попарно не сравнимые по модулю m и взаимно простые с модулем, образуют приведенную систему вычетов по модулю m.

2) Если $d(a, m) = 1$ 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 $\phi(m)$ штук. Ясно также, что все они взаимно просты с модулем, ибо $d(a, m)=1$, $d(x,m)=1 \Rightarrow d(ax, m)=1$. Значит, числа ax образуют приведенную систему вычетов.

Лемма 3. Пусть m_1 , m_2 , ..., m_k – попарно взаимно просты и $m_1 m_2 \dots m_k = M_1 m_1 = M_2 m_2 = \dots = M_k m_k$, где $M_j = m_1 \dots m_j\text{-}1\ m_j\text{+}1 \dots m_k$

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

2) Если ξ_1 , ξ_2 , ..., ξ_k пробегают приведенные системы вычетов по модулям m_1 , m_2 , ..., m_k соответственно, то значения линейной формы $M_1\xi_1 + M_2\xi_2 + \dots + M_k \xi_k$ пробегают приведенную систему вычетов по модулю $m = m_1 m_2 \dots m_k$.

Лемма 4. Пусть x_1 , x_2 , ..., x_k , x пробегают полные, а ξ_1 , ξ_2 ,..., ξ_k , ξ – пробегают приведенные системы вычетов по модулям m_1, m_2,...,m_k и $m=m_1 m_2 \dots m_k$ соответственно, где $(m_i\ m_j)=1$ при $i \neq j$. Тогда дроби $\{x_1/m_1 + x_2/m_2 + \dots + x_k/m_k\}$ совпадают с дробями $\{x/m\}$, а дроби $\{\xi_1/m_1 + \xi_2/m_2 + \dots + \xi_k/m_k\}$ совпадают с дробями $\{\xi/m\}$.

Обозначим через ε_k k -ый корень m- ой степени из единицы:

$$\varepsilon_k = \cos\frac{2\pi k}{m} + i\sin\frac{2\pi k}{m} = e^{i\frac{2\pi k}{m}}$$

Здесь $k=0,1,\dots,m\text{-}1$ – пробегает полную систему вычетов по модулю m.

Напомню, что сумма $\varepsilon_0 + \varepsilon_1 + \dots + \varepsilon_{m-1}$ всех корней m -ой степени из единицы равна нулю для любого m. Действительно, пусть $\varepsilon_0 + \varepsilon_1 + \dots + \varepsilon_{m-1} = a$. Умножим эту сумму на ненулевое число ε_1. Такое умножение геометрически в комплексной плоскости означает поворот правильного m-угольника, в вершинах которого расположены корни $\varepsilon_0 + \varepsilon_1 + \dots + \varepsilon_{m-1}$, на ненулевой угол $2\pi/m$. Ясно, что при этом корень ε_0 перейдет в корень ε_1, корень ε_1 перейдет в корень ε_2, и т.д., а корень ε_{m-1} перейдет в корень ε_0, т.е. сумма $\varepsilon_0 + \varepsilon_1 + \dots + \varepsilon_{m-1}$ не изменится. Имеем $\varepsilon_1 a = a$, откуда $a=0$.

Теорема 1. Пусть $m>0$ – целое число, $a \in \mathbf{Z}$, x пробегает полную систему вычетов по модулю m. Тогда, если a кратно m, то

$$\sum_x e^{2\pi i\frac{ax}{m}} = m$$

в противном случае, при a не кратном m,

$$\sum_x e^{2\pi i\frac{ax}{m}} = 0$$

Теорема 2. Пусть $m>0$ – целое число, ξ пробегает приведенную систему вычетов по модулю m. Тогда (сумма первообразных корней степени m):

$$\sum_{\xi} e^{2\pi i \frac{\xi}{m}} = \mu(m),$$

где $\mu(m)$ – функция Мебиуса.

Теорема Эйлера и теорема Ферма.

Теорема (Эйлера). Пусть $m>1$, $d(a,m)=1$, $\phi(m)$ – функция Эйлера. Тогда:

$$a^{\phi(m)} \equiv 1(\mathrm{mod}\ m).$$

Теорема (Ферма). Пусть p – простое число, p не делит a. Тогда:

$$a^{p-1} \equiv 1(\mathrm{mod}\ p).$$

Следствие 1. Без всяких ограничений на $a \in \mathbf{Z}$, $a^p \equiv a(\mathrm{mod}\ p)$.

Следствие 2. $(a+b)^p \equiv a^p + b^p(\mathrm{mod}\ p)$.

Пример 1. Девятая степень однозначного числа оканчивается на 7. Найти это число.

Решение. $a^9 \equiv 7(\mathrm{mod}\ 10)$ – это дано. Кроме того, очевидно, что $d(7, 10) = 1$ и $d(a, 10) = 1$. По теореме Эйлера, $a^{\phi(10)} \equiv 1(\mathrm{mod}\ 10)$. Следовательно, $a^4 \equiv 1(\mathrm{mod}\ 10)$ и, после возведения в квадрат, $a^8 \equiv 1(\mathrm{mod}\ 10)$. Поделим почленно $a^9 \equiv 7(\mathrm{mod}\ 10)$ на $a^8 \equiv 1(\mathrm{mod}\ 10)$ и получим $a \equiv 7(\mathrm{mod}\ 10)$. Это означает, что $a = 7$.

Пример 2. Доказать, что $1^{18} + 2^{18} + 3^{18} + 4^{18} + 5^{18} + 6^{18} \equiv -1(\mathrm{mod}\ 7)$.

Доказательство. Числа 1, 2, 3, 4, 5, 6 взаимно просты с 7. По теореме Ферма имеем:

$$\begin{cases} 1^6 \equiv 1(\mathrm{mod}\ 7) \\ 2^6 \equiv 1(\mathrm{mod}\ 7) \\ \quad\vdots \\ 6^6 \equiv 1(\mathrm{mod}\ 7) \end{cases}$$

Возведем эти сравнения в куб и сложим: $1^{18} + 2^{18} + 3^{18} + 4^{18} + 5^{18} + 6^{18} \equiv 6(\mathrm{mod}\ 7) \equiv -1(\mathrm{mod}\ 7)$

Пример 3. Найти остаток от деления 7^{402} на 101.

Решение. Число 101 – простое, $d(7, 101) = 1$, следовательно, по теореме Ферма: $7^{100} \equiv 1(\mathrm{mod}\ 101)$. Возведем это сравнение в четвертую степень: $7^{400} \equiv 1(\mathrm{mod}\ 101)$, домножим его на очевидное сравнение $7^2 \equiv 49(\mathrm{mod}\ 101)$, получим: $7^{402} \equiv 49(\mathrm{mod}\ 101)$. Значит, остаток от деления 7^{402} на 101 равен 49.

Пример 4. Найти две последние цифры числа 243^{402}.

Решение. Две последние цифры этого числа суть остаток от деления его на 100. Имеем: $243=200+43$; $200+43 \equiv 43(\mathrm{mod}\ 100)$ и, возведя последнее очевидное сравнение в 402-ую степень, раскроем его левую часть по биному Ньютона (мысленно, конечно). В этом гигантском выражении все слагаемые, кроме последнего, содержат степень числа 200, т.е. делятся на 100, поэтому их можно выкинуть из сравнения, после чего понятно, почему $243^{402} \equiv 43^{402}(\mathrm{mod}\ 100)$.

Далее, 43 и 100 взаимно просты, значит, по теореме Эйлера, $43^{\phi(100)} \equiv 1(\mathrm{mod}\ 100)$. Считаем: $\phi(100) = \phi(2^2 \cdot 5^2) = (10–5)(10–2) =40$.

Имеем сравнение: $43^{40} \equiv 1(\mathrm{mod}\ 100)$, которое немедленно возведем в десятую степень и умножим почленно на очевидное сравнение, проверенное на калькуляторе: $43^2 \equiv 49(\mathrm{mod}\ 100)$.

Получим:

$$\times\left[\begin{array}{l}43^{400}\equiv 1(\mathrm{mod}\,100)\\ 43^{2}\equiv 49(\mathrm{mod}\,100)\end{array}\right.$$

$$43^{402}\equiv 49(\mathrm{mod}\,100)$$

следовательно, две последние цифры числа 243^{402} суть 4 и 9.

Пример 5. Доказать, что $(73^{12} – 1)$ делится на 105.

Решение. Имеем: $105=3\cdot 5\cdot 7$, $d(73, 3) = (73, 5) = (73, 7) = 1$. По теореме Ферма:

$73^2 \equiv 1(\mathrm{mod}\ 3)$

$73^4 \equiv 1(\mathrm{mod}\ 5)$

$73^6 \equiv 1(\mathrm{mod}\ 7)$

Перемножая, получаем:

$73^{12} \equiv 1(\mathrm{mod}\ 3),(\mathrm{mod}\ 5),(\mathrm{mod}\ 7)$,

откуда, по свойствам сравнений, изложенным в пункте 16, немедленно следует: $73^{12–1} \equiv 0(\mathrm{mod}\ 105)$, ибо 105 – наименьшее общее кратное чисел 3, 5 и 7 . Именно это и требовалось.

Сравнения первой степени.

Рассмотрим сравнения первой степени вида $ax \equiv b(\mathrm{mod}\ m)$.

Как решать такое сравнение? Рассмотрим два случая.

Случай 1. Пусть a и m взаимно просты. Тогда несократимая дробь m/a сама просится разложиться в цепную дробь:

$$\frac{m}{a}=q_1+\cfrac{1}{q_2+\cfrac{1}{q_3+\cfrac{1}{\ddots\;\cfrac{\ddots}{q_{n-1}+\cfrac{1}{q_n}}}}}$$

Эта цепная дробь, разумеется, конечна, так как m/a – рациональное число. Рассмотрим две ее последние подходящие дроби:

$$\delta_{n-1}=\frac{P_{n-1}}{Q_{n-1}};\quad \delta_n=\frac{P_n}{Q_n}=\frac{m}{a}$$

Вспоминаем важное свойство числителей и знаменателей подходящих дробей: $mQ_{n-1} – aP_{n-1} = (-1)^n$. Далее (слагаемое mQ_{n-1}, кратное m, можно выкинуть из левой части сравнения):

$-aP_{n-1} \equiv (-1)^n(\mathrm{mod}\ m)$ т.е.

$aP_{n-1} \equiv (-1)^{n-1}(\mathrm{mod}\ m)$ т.е.

$a[(-1)^{n-1}P_{n-1}b] \equiv b(\mathrm{mod}\ m)$

и единственное решение исходного сравнения есть: $x \equiv (-1)^{n-1}P_{n-1}b(\mathrm{mod}\ m)$

Пример. Решить сравнение $111x \equiv 75(\mathrm{mod}\ 322)$.

Решение. $d(111, 322) = 1$. Включаем алгоритм Евклида:

$322=111\cdot \underline{2}+100$

$111=100\cdot \underline{1}+11$

$100=11\cdot \underline{9}+1$

$11=1\cdot \underline{11}$

(В равенствах подчеркнуты неполные частные.) Значит, $n=4$, а соответствующая цепная дробь такова:

$$\frac{m}{a} = \frac{322}{111} = 2 + \cfrac{1}{1 + \cfrac{1}{9 + \cfrac{1}{11}}}$$

Посчитаем числители подходящих дробей, составив для этого стандартную таблицу:

	0	2	1	9	11
P_n	1	2	3	29	322

Числитель предпоследней подходящей дроби равен 29, следовательно, готовая формула дает ответ: $x \equiv (-1)^3 \cdot 29 \cdot 75 \equiv -2175 \equiv 79 (mod\ 322)$.

Случай 2. Пусть НОД$(a, m) = d$. В этом случае, для разрешимости сравнения $ax \equiv b(mod\ m)$ необходимо, чтобы d делило b, иначе сравнение вообще выполняться не может.

Действительно, $ax \equiv b(\text{mod}\ m)$ бывает тогда, и только тогда, когда $ax - b$ делится на m нацело, т.е. $ax - b = t \cdot m,\ t \in \mathrm{Z}$, откуда $b = ax - tm$, а правая часть последнего равенства кратна d.

Пусть $b=db_1,\ a=da_1,\ m=dm_1$. Тогда обе части сравнения $xa_1d \equiv b_1d(mod\ m_1d)$ и его модуль поделим на d: $xa_1 \equiv b_1(mod\ m_1)$, где уже a_1 и m_1 взаимно просты. Согласно случаю 1 этого пункта, такое сравнение имеет единственное решение x_0:

$$x \equiv x_0\ (mod\ m_1)\ \textbf{(*)}$$

По исходному модулю m, числа (*) образуют столько решений исходного сравнения, сколько чисел вида (*) содержится в полной системе вычетов: 0,1,2,..., m-2, m-1. Очевидно, что из чисел $x = x_0 + tm$ в полную систему наименьших неотрицательных вычетов попадают только $x_0,\ x_0+m_1,\ x_0+2m_1, \ldots,\ x_0+(d-1)m_1$, т.е. всего d чисел. **Значит у исходного сравнения имеется *d* решений**.

Подведем итог рассмотренных случаев в виде следующей теоремы:

Теорема 1. Пусть НОД$(a,m) = d$. Если b не делится на d, сравнение $ax \equiv b(\text{mod}\ m)$ не имеет решений. Если b кратно d, сравнение $ax \equiv b(\text{mod}\ m)$ имеет d штук решений.

Пример. Решить сравнение $111x \equiv 75(\text{mod}\ 321)$.

Решение. НОД(111, 321) = 3, поэтому поделим сравнение и его модуль на 3:

$$37x \equiv 25(\text{mod}\ 107) \text{ и уже НОД}(37, 107) = 1.$$

Включаем алгоритм Евклида (как обычно, подчеркнуты неполные частные):

$$107=37 \cdot \underline{2}+33$$
$$37=33 \cdot \underline{1}+4$$
$$33=4 \cdot \underline{8}+1$$
$$4=1 \cdot \underline{4}$$

Имеем $n = 4$ и цепная дробь такова:

$$\frac{m}{a} = \frac{107}{37} = 2 + \cfrac{1}{1 + \cfrac{1}{8 + \cfrac{1}{4}}}$$

Таблица для нахождения числителей подходящих дробей:

q_n	0	2	1	8	4
P_n	1	2	3	26	107

Значит, $x \equiv (-1)^3 \cdot 26 \cdot 25 \equiv -650(\text{mod } 107) \equiv -8(\text{mod } 107) \equiv 99(\text{mod } 107)$.

Три решения исходного сравнения:

$$x \equiv 99(\text{mod } 321),\ x \equiv 206(\text{mod } 321),\ x \equiv 313(\text{mod } 321),$$

и других решений нет.

Теорема 2. Пусть $m > 1$, НОД$(a, m) = 1$. Тогда сравнение $ax \equiv b(\text{mod } m)$ имеет решение: $x \equiv ba^{\phi(m)-1}(\text{mod } m)$.

Пример. Решить сравнение $7x \equiv 3(\text{mod } 10)$. Вычисляем: $\phi(10) = 4$; $x \equiv 3 \cdot 7^{4-1}(\text{mod } 10) \equiv 1029(\text{mod } 10) \equiv 9(\text{mod } 10)$.

Видно, что этот способ решения сравнений хорош (в смысле минимума интеллектуальных затрат на его осуществление), но может потребовать возведения числа a в довольно большую степень, что довольно трудоемко. Для того чтобы как следует это прочувствовать, возведите самостоятельно число 24789 в степень 46728.

Теорема 3. Пусть p – простое число, $0<a<p$. Тогда сравнение $ax \equiv b(\text{mod } p)$ имеет решение:

$$x \equiv b\cdot(-1)^{a-1}\cdot\frac{(p-1)(p-2)\dots(p-a+1)}{1\cdot2\cdot3\cdot\dots\cdot(a-1)\cdot a}(\text{mod}\, p) \equiv$$

$$\equiv b\cdot(-1)^{a-1}\cdot\frac{(p-1)!}{(a!)\cdot(p-a)!}(\text{mod}\, p) \equiv b\cdot(-1)^{a-1}\cdot\frac{p!}{p\cdot(a!)\cdot(p-a)!}(\text{mod}\, p) \equiv$$

$$\equiv b\cdot(-1)^{a-1}\cdot\frac{1}{p}\cdot C_p^a(\text{mod}\, p),$$

где C_p^a – биномиальный коэффициент.

Пример. Решить сравнение $7x \equiv 2(\text{mod } 11)$. Вычисляем:

$$C_{11}^7 = \frac{11!}{(7!)\cdot(11-7)!} = \frac{8\cdot9\cdot10\cdot11}{2\cdot3\cdot4} = 2\cdot3\cdot5\cdot11 = 330;$$

$$x \equiv 2\cdot(-1)^6\cdot\frac{1}{11}\cdot330 \equiv 60 \equiv 5(\text{mod} 11)$$

Лемма 1 (Китайская теорема об остатках). Пусть дана простейшая система сравнений первой степени:

$$\begin{cases} x \equiv b_1(\text{mod}\, m_1) \\ x \equiv b_2(\text{mod}\, m_2) \\ \quad\vdots \\ x \equiv b_k(\text{mod}\, m_k), \end{cases} \qquad (*)$$

где $m_1, m_2, \dots, m_k$ попарно взаимно просты. Пусть, далее, $m_1\, m_2 \dots m_k = M_s\, m_s$; $M_s\, M_s^{\nabla} \equiv 1(mod\ m_s)$. (Очевидно, что такое число M_s^{∇} всегда можно подобрать хотя бы с помощью алгоритма Евклида, т.к. $(m_s, M_s)=1$); $x_0 = M_1M_1^{\nabla}b_1 + M_2M_2^{\nabla}b_2 + \dots + M_kM_k^{\nabla}b_k$. Тогда система (*) равносильна одному сравнению $x \equiv x_0\ (mod\ m_1\, m_2 \dots m_k)$, т.е. набор решений (*) совпадает с набором решений сравнения $x \equiv x_0\ (mod\ m_1\, m_2 \dots m_k)$.

Пример. Однажды средний товарищ подошел к умному товарищу и попросил его найти число, которое при делении на 4 дает в остатке 1, при делении на 5 дает в остатке 3, а при делении на 7 дает в остатке 2. Сам средний товарищ искал такое число уже две недели. Умный товарищ тут же составил систему:

$$\begin{cases} x \equiv 1(\mathrm{mod}\,4) \\ x \equiv 3(\mathrm{mod}\,5) \\ x \equiv 2(\mathrm{mod}\,7), \end{cases}$$

которую начал решать, пользуясь леммой 1. Вот его решение:
$b_1 = 1$; $b_2 = 3$; $b_3 = 2$; $m_1\, m_2\, m_3$, т.е. $M_1 = 35$, $M_2 = 28$, $M_3 = 20$.
Далее он нашел:

$$35 \cdot 3 = 1(\mathrm{mod}\ 4)$$
$$28 \cdot 2 = 1(\mathrm{mod}\ 5)$$
$$20 \cdot 6 = 1(\mathrm{mod}\ 7)$$

т.е. $M_1^{\nabla} = 3$, $M_2^{\nabla} = 2$, $M_3^{\nabla} = 6$. Значит $x_0 = 35 \cdot 3 \cdot 1 + 28 \cdot 2 \cdot 3 + 20 \cdot 6 \cdot 2 = 513$. После этого, по лемме 1, умный товарищ сразу получил ответ:

$$x \equiv 513(\mathrm{mod}\ 140) \equiv 93(\mathrm{mod}\ 140),$$

т.е. наименьшее положительное число, которое две недели искал средний товарищ, равно 93. Так умный товарищ в очередной раз помог среднему товарищу.

Лемма 2. Если b_1, $b_2,\dots,b_k$ пробегают полные системы вычетов по модулям m_1, $m_2,\dots,m_k$ соответственно, то x_0 пробегает полную систему вычетов по модулю $m_1\, m_2 \dots m_k$.