Решение задач по теории чисел

О.В. Митина

1 Сравнения первой степени с одним неизвестным $ax \equiv b \pmod m$

Пример 1. Решите сравнение

$$1287x \equiv 447 \pmod{516}. \tag{1}$$

Решение:
1) Заменим коэффициенты сравнения (1) соответствующими наименьшими положительными вычетами по модулю 516, получим:

$$255x \equiv 447 \pmod{516}. \tag{2}$$

2) Если наибольший общий делитель (a, m) чисел a и m равен d и d делит b, то сравнение $ax \equiv b \pmod m$ имеет d решений. Если же d не делит b, то сравнение $ax \equiv b \pmod m$ не имеет решений. Для сравнения (2) имеем $d = (a, m) = (255, 516) = 3$. Поскольку $d = 3$ делит $b = 447$, то сравнение (2), а, значит, и сравнение (1) имеет 3 решения.
3) Разделим обе части сравнения (2) и его модуль на $d = 3$, получим:

$$85x \equiv 149 \pmod{172}. \tag{3}$$

Рассмотрим два способа решения сравнения $ax \equiv b \pmod m$, где $(a, m) = 1$.
Первый способ:
Решение x_0 находим по формуле

$$x_0 \equiv (-1)^{n-1} P_{n-1} b \pmod m,$$

где P_{n-1} – числитель предпоследней подходящей дроби для числа $\frac{m}{a}$, разложенного в непрерывную (цепную) дробь. Разложим число $\frac{172}{85}$ в непрерывную дробь и найдем числитель предпоследней подходящей дроби:

$$\frac{172}{85} = 2 + \frac{2}{85} = 2 + \frac{1}{42 + \frac{1}{2}} = q_1 + \frac{1}{q_2 + \frac{1}{q_3}}.$$

Найдем числители подходящих дробей по рекуррентной формуле

$$P_{i+1} = q_i P_i + P_{i-1},$$

где $P_0 = 1, P_1 = q_1$, $i = 1, ..., n-1$:

i	0	1	2	3
q_i		2	42	2
P_i	1	2	85	172

Получим, что $n = 3$, $P_{n-1} = P_2 = 85$ и решение сравнения (2) имеет вид:

$$x_0 \equiv (-1)^{n-1} P_{n-1} b \pmod m \equiv (-1)^{3-1} \cdot 85 \cdot 149 \pmod{172} \equiv$$
$$\equiv 85 \cdot (-23) \pmod{172} \equiv -1955 \pmod{172} \equiv 109 \pmod{172}.$$

Второй способ:
По теореме Эйлера для чисел a и m, удовлетворяющих условию $(a, m) = 1$, выполняется сравнение $a^{\varphi(m)} \equiv 1 \pmod{m}$, где $\varphi(m)$ - функция Эйлера. Поэтому решение x_0 сравнения $ax \equiv b \pmod{m}$ можно найти по формуле

$$x_0 \equiv b \cdot a^{\varphi(m)-1} \pmod{m}.$$

Найдем $\varphi(172)$. Поскольку $172 = 2^2 \cdot 43$, то по свойствам функции Эйлера $\varphi(172) = \varphi(2^2) \cdot \varphi(43) = (2^2 - 2^1) \cdot (43 - 1) = 2 \cdot 42 = 84$. Тогда

$$\begin{aligned} x_0 &\equiv 149 \cdot 85^{84-1} \pmod{172} \equiv -23 \cdot 85^{2 \cdot 41+1} \pmod{172} \equiv \\ &\equiv -23 \cdot 85 \cdot (85^2)^{41} \pmod{172} \equiv -1955 \cdot (25 \cdot 289)^{41} \pmod{172} \equiv \\ &\equiv 109 \cdot (25 \cdot (-55))^{41} \pmod{172} \equiv 109 \cdot 1^{41} \pmod{172} \equiv 109 \pmod{172}. \end{aligned}$$

4) Итак, $x_0 \equiv 109 \pmod{172}$ является решением сравнения (3). Все решения сравнения (2), а также сравнения (1), находят по формуле

$$x = x_0 + 172 \cdot k, \text{ где } k = 0, 1, ..., d - 1.$$

В нашем случае $k = 0, 1, 2$, значит,

$$x \equiv 109; 281; 453 \pmod{516}.$$

Ответ: $x \equiv 109; 281; 453 \pmod{516}$.

2 Решение систем сравнений первой степени с одним неизвестным

Пример 2. Решите систему сравнений

$$\begin{cases} 13x \equiv 7 \pmod{24}, \\ 8x \equiv 5 \pmod{75}. \end{cases} \tag{1}$$

Решение.

Решив каждое из сравнений системы (1) отдельно (см. пример 1), получим систему

$$\begin{cases} x \equiv 19 \pmod{24}, \\ x \equiv 10 \pmod{75}. \end{cases} \tag{2}$$

Используя каноническое разложение модулей $24 = 2^3 \cdot 3$, $75 = 3 \cdot 5^2$, получим что система (2) равносильна системе

$$\begin{cases} x \equiv 19 \pmod{8}, \\ x \equiv 19 \pmod{3}, \\ x \equiv 10 \pmod{25}, \\ x \equiv 10 \pmod{3} \end{cases}$$

или

$$\begin{cases} x \equiv 3 \pmod{8}, \\ x \equiv 1 \pmod{3}, \\ x \equiv 10 \pmod{25}, \\ x \equiv 1 \pmod{3}. \end{cases}$$

Второе и четвертое сравнения системы одинаковые, поэтому удалим одно из них. Получим систему, у которой модули всех сравнений попарно взаимно просты

$$\begin{cases} x \equiv 3 \pmod{8}, \\ x \equiv 1 \pmod{3}, \\ x \equiv 10 \pmod{25}. \end{cases} \tag{3}$$

Для решения системы (3) воспользуемся формулой, следующей из китайской теоремы об остатках. Для системы сравнений

$$\begin{cases} x \equiv b_1 \pmod{m_1}, \\ x \equiv b_2 \pmod{m_2}, \\ \qquad \dots \\ x \equiv b_n \pmod{m_n}, \end{cases}$$

где числа $m_1, m_2, \dots, m_n$ попарно взаимно просты, решение находится по следующей формуле

$$x \equiv M_1 M_1' b_1 + M_2 M_2' b_2 + \ldots + M_n M_n' b_n \pmod{m}, \tag{4}$$

где $m = m_1 \cdot m_2 \cdot \ldots \cdot m_n$, $M_i = \frac{m}{m_i}$, M_i' – некоторое решение сравнения $M_i x \equiv 1 \pmod{m_i}$, $i = 1, \dots, n$.

Для системы (3) имеем $m = 8 \cdot 3 \cdot 25 = 600$, $M_1 = \frac{8 \cdot 3 \cdot 25}{8} = 75$, $M_2 = \frac{8 \cdot 3 \cdot 25}{3} = 200$, $M_3 = \frac{8 \cdot 3 \cdot 25}{25} = 24$.

Найдем M_i', $i = 1, 2, 3$:

$$\begin{aligned}
75x \equiv 1 \pmod 8 &\Leftrightarrow 3x \equiv 1 \pmod 8 \Leftrightarrow x \equiv 3 \pmod 8 \Rightarrow M_1' = 3,\\
200x \equiv 1 \pmod 3 &\Leftrightarrow 2x \equiv 1 \pmod 3 \Leftrightarrow x \equiv 2 \pmod 3 \Rightarrow M_2' = 2,\\
24x \equiv 1 \pmod{25} &\Leftrightarrow x \equiv -1 \pmod{25} \Rightarrow M_3' = -1.
\end{aligned}$$

Подставим значения M_i, M_i', b_i в формулу (4):

$$\begin{aligned}
x &\equiv M_1 \cdot M_1' \cdot b_1 + M_2 \cdot M_2' \cdot b_2 + M_3 \cdot M_3' \cdot b_3 =\\
&= 75 \cdot 3 \cdot 3 + 200 \cdot 2 \cdot 1 + 24 \cdot (-1) \cdot 10 =\\
&= 675 + 400 - 240 = 835 \equiv 235 \pmod{600}.
\end{aligned}$$

В качестве проверки убеждаемся, что 235 при делении на 8 дает в остатке 3, при делении на 3 дает в остатке 1 и при делении на 25 дает в остатке 10, т.е. действительно является решением системы (3), а, значит, и решением системы (1).

Ответ: $x \equiv 235 \pmod{600}$.

3 Сравнения произвольной степени с одним неизвестным $f(x) \equiv 0 \pmod m$

Пусть $m = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$ – каноническое разложение числа $m > 0$. Тогда сравнение

$$f(x) \equiv 0 \pmod m \tag{1}$$

равносильно системе сравнений

$$\begin{cases} f(x) \equiv 0 \pmod{p_1^{\alpha_1}}, \\ f(x) \equiv 0 \pmod{p_2^{\alpha_2}}, \\ \qquad \ldots \\ f(x) \equiv 0 \pmod{p_k^{\alpha_k}}. \end{cases}$$

Таким образом, решение сравнения (1) сводится к решению нескольких сравнений вида

$$f(x) \equiv 0 \pmod{p^\alpha}. \tag{2}$$

Из решений $x \equiv x_1 \pmod p$ сравнения $f(x) \equiv 0 \pmod p$ выбираем решения сравнения (2) вида

$$x \equiv x_\alpha + p^\alpha t_\alpha, \quad t_\alpha \in \mathbb{Z}$$

или

$$x \equiv x_\alpha \pmod{p^\alpha}.$$

Эти решения определяются последовательно для $s = 2, 3, \ldots, \alpha$ в виде $x_s + p^s t_s$, где t_s – решение сравнения

$$f(x_{s-1}) + f'(x_{s-1}) p^{s-1} t \equiv 0 \pmod{p^s}$$

или

$$\frac{f(x_{s-1})}{p^{s-1}} + f'(x_{s-1}) t \equiv 0 \pmod p. \tag{3}$$

Поскольку x_{s-1} является решением сравнения $f(x) \equiv 0 \pmod{p^{s-1}}$, то $\frac{f(x_{s-1})}{p^{s-1}}$ является целым числом. Если $p \nmid f'(x_{s-1})$, то сравнение (3) имеет единственное решение. Если $p \mid f'(x_{s-1})$, то сравнение (3) имеет p решений при условии $p \mid \frac{f(x_{s-1})}{p^{s-1}}$, иначе сравнение (3) не имеет решений.

Пример 3. Решите сравнение

$$5x^3 + 4x^2 + 8x + 18 \equiv 0 \pmod{135}.$$

Решение.

Шаг 1. Обозначим $f(x) = 5x^3 + 4x^2 + 8x + 18$. Поскольку $135 = 5 \cdot 3^3$, то данное сравнение равносильно системе

$$\begin{cases} f(x) \equiv 0 \pmod 5, \\ f(x) \equiv 0 \pmod{27}. \end{cases} \tag{4}$$

Шаг 2. Решим сравнение по модулю 5. Рассмотрим полную систему абсолютно наименьших вычетов по модулю 5. Кроме того, удобно заменить

коэффициенты многочлена $f(x)$ на соответствующие абсолютно наименьшие вычеты по модулю 5:

$$f(x) = 5x^3 + 4x^2 + 8x + 18 \equiv -x^2 - 2x - 2 \pmod 5.$$

Итак,

$$\begin{aligned} f(-2) &= -(-2)^2 - 2\cdot(-2) - 2 = -2 \not\equiv 0 \pmod 5,\\ f(-1) &= -(-1)^2 - 2\cdot(-1) - 2 = -1 \not\equiv 0 \pmod 5,\\ f(0) &= -0^2 - 2\cdot 0 - 2 = -2 \not\equiv 0 \pmod 5,\\ f(1) &= -1^2 - 2\cdot 1 - 2 = -5 \equiv 0 \pmod 5,\\ f(2) &= -2^2 - 2\cdot 2 - 2 = -10 \equiv 0 \pmod 5. \end{aligned}$$

Получили, что сравнение $f(x) \equiv 0 \pmod 5$ имеет два решения

$$x \equiv 1; 2 \pmod 5.$$

Шаг 3. Далее, для решения сравнения $f(x) \equiv 0 \pmod{27}$ найдем сначала решения сравнения $f(x) \equiv 0 \pmod 3$. Из них выберем решения сравнения $f(x) \equiv 0 \pmod 9$, а затем из решений сравнения по модулю 9 найдем решения сравнения $f(x) \equiv 0 \pmod{27}$.

Модуль 3. *Все вычисления производятся по модулю 3.*

$$\begin{aligned} f(x) &= 5x^3 + 4x^2 + 8x + 18 \equiv 2x^3 + x^2 + 2x \pmod 3,\\ f'(x) &= 15x^2 + 8x + 8 \equiv 2x + 2 \pmod 3. \end{aligned}$$

Имеем

$$\begin{aligned} f(0) &= 2\cdot 0^3 + 0^2 + 2\cdot 0 \equiv 0 \pmod 3,\\ f(1) &= 2\cdot 1^3 + 1^2 + 2\cdot 1 = 2 \not\equiv 0 \pmod 3,\\ f(2) &= 2\cdot 2^3 + 2^2 + 2\cdot 2 = 24 \equiv 0 \pmod 3. \end{aligned}$$

Получили, что сравнение $f(x) \equiv 0 \pmod 3$ имеет два решения $x \equiv 0 \pmod 3$, $x \equiv 2 \pmod 3$. Если $f(x) \equiv 0 \pmod 9$ имеет решения, то эти решения имеют вид $0 + 3t$ или $2 + 3t$ для некоторого $t \in \mathbb{Z}$.

Модуль 9. *Все вычисления производятся по модулю 9.*

$$\begin{aligned} f(x) &= 5x^3 + 4x^2 + 8x + 18,\\ f'(x) &= 15x^2 + 8x + 8. \end{aligned}$$

Используем формулу (3) при $s = 2$:

$$f(x_1) + f'(x_1)pt \equiv 0 \pmod{p^2}$$

или

$$\frac{f(x_1)}{p} + f'(x_1)t \equiv 0 \pmod p. \tag{5}$$

1) Рассмотрим $x_1 \equiv 0 \pmod 3$, т.е. $x_1 = 0 + 3t$. Имеем

$$\begin{aligned} f(x_1) = f(0) &= 5\cdot 0^3 + 4\cdot 0^2 + 8\cdot 0 + 18 = 18 \equiv 0 \pmod 9,\\ f'(x_1) = f'(0) &= 15\cdot 0^2 + 8\cdot 0 + 8 = 8 \equiv -1 \pmod 9. \end{aligned}$$

По формуле (5) получим $\frac{0}{3} + (-1) \cdot t \equiv 0 \pmod 3$ или $t \equiv 0 \pmod 3$. Поэтому $t_1 = 0$ и $x_2 = x_1 + 3t_1 = 0 + 3 \cdot 0 = 0$ является решением сравнения $f(x) \equiv 0 \pmod 9$.

2) Те же действия выполним для $x_1 \equiv 2 \pmod 3$, т.е. $x_1 = 2 + 3t$. Имеем

$$f(x_1) = f(2) = 5 \cdot 2^3 + 4 \cdot 2^2 + 8 \cdot 2 + 18 = 90 \equiv 0 \pmod 9,$$
$$f'(x_1) = f'(2) = 15 \cdot 2^2 + 8 \cdot 2 + 8 = 84 \equiv 3 \pmod 9,$$

По формуле (5) получим $\frac{0}{3} + 3 \cdot t \equiv 0 \pmod 3$ или $0 \equiv 0 \pmod 3$. Поэтому $t_1 = 0; 1; 2$ и числа $x_2 = x_1 + 3t_1 = 2 + 3t_1 = 2; 5; 8$ являются решениями сравнения $f(x) \equiv 0 \pmod 9$.

Модуль 27. *Все вычисления производятся по модулю 27.*

$$f(x) = 5x^3 + 4x^2 + 8x + 18,$$
$$f'(x) = 15x^2 + 8x + 8.$$

Используем формулу (3) при $s = 3$:

$$f(x_2) + f'(x_2)p^2t \equiv 0 \pmod{p^3}$$

или

$$\frac{f(x_2)}{p^2} + f'(x_2)t \equiv 0 \pmod p. \tag{6}$$

Рассмотрим $x_2 \equiv 0; 2; 5; 8 \pmod 9$, т.е. $x_2 = 0 + 9t$, $x_2 = 2 + 9t$, $x_2 = 5 + 9t$, $x_2 = 8 + 9t$.

1) Для $x_2 = 0 + 9t$ имеем

$$f(x_2) = f(0) = 5 \cdot 0^3 + 4 \cdot 0^2 + 8 \cdot 0 + 18 \equiv 18 \pmod{27},$$
$$f'(x_2) = f'(0) = 15 \cdot 0^2 + 8 \cdot 0 + 8 \equiv 8 \pmod{27}.$$

По формуле (6) получим $\frac{18}{9} + 8 \cdot t \equiv 0 \pmod 3$ или $t \equiv 2 \pmod 3$. Поэтому $t_2 = 2$ и

$$x_3 = x_2 + 9t_2 = 0 + 9 \cdot 2 = 18$$

является решением сравнения $f(x) \equiv 0 \pmod{27}$.

2) Для $x_2 = 2 + 9t$ имеем
$f(x_2) = f(2) = 90 \equiv 9 \pmod{27}$,
$f'(x_2) = f'(2) = 84 \equiv 3 \pmod{27}$, $\frac{9}{9} + 3 \cdot t \equiv 0 \pmod 3$ или $1 \not\equiv 0 \pmod 3$.
Среди чисел вида $2 + 9t$ нет решений сравнения $f(x) \equiv 0 \pmod{27}$.

3) Для $x_2 = 5 + 9t$ имеем
$f(x_2) = f(5) = 783 \equiv 0 \pmod{27}$,
$f'(x_2) = f'(5) = 423 \equiv 18 \pmod{27}$, $\frac{0}{9} + 18t \equiv 0 \pmod 3$ или $0 \equiv 0 \pmod 3$.
Поэтому $t_2 = 0; 1; 2$ и

$$x_3 = 5 + 9t_2 = 5; 14; 23$$

являются решениями сравнения $f(x) \equiv 0 \pmod{27}$.

4) Для $x_2 = 8 + 9t$ имеем
$f(x_2) = f(8) = 2898 \equiv 9 \pmod{27}$,
$f'(x_2) = f'(8) = 1032 \equiv 6 \pmod{27}$, $\frac{9}{9} + 6t \equiv 0 \pmod 3$ или $1 \not\equiv 0 \pmod 3$.
Среди чисел вида $8 + 9t$ нет решений сравнения $f(x) \equiv 0 \pmod{27}$.

Шаг 4. Итак, система (4) решена:

$$\begin{cases} x & \equiv & 1;2 \pmod 5, \\ x & \equiv & 5;14;18;23 \pmod{27}. \end{cases}$$

В правой части сравнений находятся несколько значений, поэтому удобно рассматривать систему

$$\begin{cases} x & \equiv & b_1 \pmod 5, \\ x & \equiv & b_2 \pmod{27}, \end{cases} \quad \text{где } b_1 \in \{1;2\},\ b_2 \in \{5;14;18;23\}.$$

Воспользуемся формулой, следующей из китайской теоремы об остатках (см. пример 2):

$m = 5 \cdot 27 = 135$,

$$M_1 = \frac{m}{5} = 27, \quad 27x \equiv 1 \pmod 5 \Leftrightarrow x \equiv 3 \pmod 5 \Rightarrow M_1' = 3;$$
$$M_2 = \frac{m}{27} = 5, \quad 5x \equiv 1 \pmod{27} \Leftrightarrow x \equiv 11 \pmod{27} \Rightarrow M_2' = 11;$$

$$x \equiv M_1 \cdot M_1' \cdot b_1 + M_2 \cdot M_2' \cdot b_2 \pmod{135} \equiv$$
$$\equiv 27 \cdot 3 \cdot b_1 + 5 \cdot 11 \cdot b_2 \pmod{135} \equiv 81b_1 + 55b_2 \pmod{135}.$$

Подставляя $b_1 = 1;2$ и $b_2 = 5;14;18;23$, получим все решения исходного сравнения

$$x \equiv 32;41;72;77;86;122;126;131 \pmod{135}.$$

Ответ: $x \equiv 32;41;72;77;86;122;126;131 \pmod{135}$.