Лекция 7

СРАВНЕНИЯ С НЕИЗВЕСТНОЙ ВЕЛИЧИНОЙ

Решение алгебраических сравнений

- ***Пусть многочлены*** $f(x), g(x) \in Z[x]$
- ***Будем рассматривать сравнения вида***

$$f(x) \equiv g(x) (\mathrm{mod}\, m)$$

- ***Такие сравнения называют алгебраическими***

- ***Если в такое сравнение вместо*** x ***подставлять различные целые числа, то некоторые из них могут удовлетворять сравнению, то есть при их подстановке вместо*** x ***получается верное числовое сравнение***

Теорема 1

Если число c удовлетворяет сравнению

$$f(x) \equiv g(x) \pmod{m}, \qquad (1)$$

то и весь класс $\overline{c}$ ***по модулю m состоит из чисел, удовлетворяющих этому сравнению***

Доказательство

- ***Пусть*** $b \equiv c \pmod{m}$
- ***Тогда*** $b^k \equiv c^k \pmod{m}$, ***k = 0, 1, 2, …***
- $a_k b^k \equiv a_k c^k \pmod{m}$
- ***Складывая такие сравнения, получим, что***

$$f(b) \equiv f(c) \pmod{m} \qquad g(b) \equiv g(c) \pmod{m}$$

- ***А так как по условию*** $f(c) \equiv g(c) \pmod{m}$ ***, то по транзитивности*** $f(b) \equiv g(b) \pmod{m}$ ***и*** b ***удовлетворяет (1)***
- ***Таким образом вместе с*** c ***любое число*** b ***класса*** $\overline{c}$ ***тоже удовлетворяет сравнению (1)***

Определение

Решением сравнения

$$f(x) \equiv g(x) (\mathrm{mod}\, m), \qquad (1)$$

называется класс чисел по модулю m, удовлетворяющих этому сравнению

- ***Числом решений сравнения называют число классов чисел, удовлетворяющих сравнению***
- ***Так как классов по модулю m конечное число, то для решения сравнения (1) достаточно взять полную систему вычетов по модулю m и отобрать те классы, представители которых удовлетворяют (1)***

Примеры

1. $x^3 - 2x + 6 \equiv 0 (\mathrm{mod}\, 11)$

Непосредственная проверка показывает, что в полной системе наименьших по абсолютной величине вычетов –5, –4, –3, –2, –1, 0, 1, 2, 3, 4, 5 сравнению удовлетворяет только одно число 5

Решение записываем в виде $x \equiv 5 (\mathrm{mod}\, 11)$

2. $x^4 + 2x^2 + 6 \equiv 0 (\mathrm{mod}\, 8)$

В полной системе вычетов –3, –2, –1, 0, 1, 2, 3, 4 ни одно число не удовлетворяет сравнению и, следовательно, сравнение не имеет решений

3. $x^3 - x \equiv 0 (\mathrm{mod}\, 3)$

Этому сравнению удовлетворяет любое число (по теореме Ферма). Сравнение имеет 3 решения – классы

$\overline{0}, \overline{1}, \overline{2}$

Равносильные сравнения

Определение

Пусть $f(x),\ g(x), f_1(x), g_1(x) \in Z[x]$

Сравнения $f(x) \equiv g(x) (\mathrm{mod}\, m)$ ***и*** $f_1(x) \equiv g_1(\mathrm{mod}\, m_1)$

называются равносильными (эквивалентными), если множества чисел, удовлетворяющих этим сравнениям, совпадают

Теорема 2

1) ***Если к обеим частям сравнения*** $f(x) \equiv g(x) \pmod m$ ***прибавим любой многочлен*** $\varphi(x) \in Z[x]$ ***, то получим сравнение, равносильное первоначальному***
2) ***Если обе части сравнения*** $f(x) \equiv g(x) \pmod m$ ***умножим на одно и то же число, взаимно простое с модулем, то получим сравнение, равносильное первоначальному***
3) ***Если обе части сравнения и модуль умножим на одно и то же натуральное число, то получим сравнение, равносильное первоначальному.***

Из теоремы 2 (пункт 1) следует, что сравнение

$$f(x) \equiv g(x) \pmod m$$

можно заменить равносильным сравнением

$$f(x) - g(x) \equiv 0 \pmod m$$

Поэтому в дальнейшем достаточно рассматривать сравнение

$$F(x) \equiv 0 \pmod m \quad (F(x) = f(x) - g(x))$$

Теорема 3

Пусть $f(x)=a_0+a_1x+\ldots+a_nx^n$ ***и*** $g(x)=b_0+b_1x+\ldots+b_nx^n$ **–**

многочлены с целыми коэффициентами.

Если $a_0\equiv b_0(\mathrm{mod}\,m)$, $a_1\equiv b_1(\mathrm{mod}\,m)$, **…,** $a_n\equiv b_n(\mathrm{mod}\,m)$ **, то**

сравнения $f(x)\equiv 0(\mathrm{mod}\,m)$ ***и*** $g(x)\equiv 0(\mathrm{mod}\,m)$ ***равносильны.***

Из теоремы следует, что сравнение заменится равносильным, если отбросить или добавить слагаемые с коэффициентами, кратными модулю

Пример

Сравнения $17x^{15}+20x^{10}+12x^5+6x^4+1\equiv 0(\mathrm{mod}\,3)$ и

$2x^{15}-x^{10}+1\equiv 0(\mathrm{mod}\,3)$ равносильны, так как

$17\equiv 2,\ 20\equiv -1,\ 12\equiv 0,\ 6\equiv 0$ по модулю 3

Определение

Степенью сравнения $f(x) \equiv 0 (\mathrm{mod}\, m)$ ***называют степень многочлена*** $f(x)$ ***, если старший коэффициент*** $f(x)$ ***не делится на m***

Пример

Степень сравнения $14x^{12} - 35x^7 + 10x^2 - 3 \equiv 0 (\mathrm{mod}\, 7)$ *равна двум, так как* $14 \not\vdots 7, -35 \not\vdots 7$ *, а само сравнение равносильно*

$$3x^2 - 3 \equiv 0 (\mathrm{mod}\, 7)$$

Лекция 8

СРАВНЕНИЯ ПЕРВОЙ СТЕПЕНИ

Сравнения 1-ой степени

Сравнение 1-ой степени может быть приведено к виду

$$ax \equiv b(\mathrm{mod}\, m) \qquad (2)$$

Теорема 4

Если $(a,m)=1$***, то сравнение (2) имеет единственное решение***

Теорема 5

Если $(a,m)=1$***, то решением сравнения (2) является класс***

$$x_0 \equiv a^{\varphi(m)-1} \cdot b(\mathrm{mod}\, m)$$

Методы решений сравнения

$$ax \equiv b (\mathrm{mod}\, m) \qquad (2)$$

1. *Метод подбора*
2. *Использование теоремы Эйлера*
3. *Метод преобразования коэффициентов*

Теорема 6

Если $(a,m)=d$ ***и*** b ***не делится на*** d***, то сравнение*** **(2)** ***не имеет решений***

Теорема 7

Если $(a,m)=d,\ d>1$ ***и*** $b \vdots d$ ***, то сравнение*** **(2)** ***имеет*** d ***решений, которые составляют один класс вычетов по модулю*** $\frac{m}{d}$ ***и находятся по формулам***

$$x_0 \equiv c \pmod{m},\quad x_1 \equiv c+\frac{m}{d} \pmod{m},$$

$$x_2 \equiv c+2\frac{m}{d} \pmod{m},\ \ldots,\quad x_{d-1} \equiv c+(d-1)\frac{m}{d} \pmod{m},$$

где c ***удовлетворяет вспомогательному сравнению***

$$\frac{a}{d}x \equiv \frac{b}{d}\left(\mathrm{mod}\,\frac{m}{d}\right).$$

Алгоритм решения сравнения

$$ax \equiv b (\mathrm{mod}\, m) \qquad (2)$$

1) ***Убедившись, что*** $(a,m) = d,\ d > 1$ ***и*** $b \vdots d$ ***, делим обе части и модуль сравнения (2) на*** d ***и получаем вспомогательное сравнение***

$$a_1 x \equiv b_1 (\mathrm{mod}\, m_1),\ \textbf{где}\ a_1 = \frac{a}{d},\ b_1 = \frac{b}{d},\ m_1 = \frac{m}{d}$$

Сравнение имеет единственное решение.

Пусть $\bar{c}$ ***– это решение***

2) ***Записываем ответ***

$$x_0 \equiv c (\mathrm{mod}\, m),\ \ x_1 \equiv c + m_1 (\mathrm{mod}\, m),$$

$$x_2 \equiv c + 2m_1 (\mathrm{mod}\, m), \ldots,\ x_{d-1} \equiv c + (d-1)m_1 (\mathrm{mod}\, m).$$

Неопределённые уравнения

Диофантово уравнение первой степени с двумя неизвестными $ax+by=c$ *, где* $a,b,c\in Z$

Требуется решить это уравнение в целых числах

- **Если** $(a,b)=d$ **и** c **не делится на** d**, то очевидно, что сравнение не имеет решений в целых числах**
- **Если же** c **делится на** d**, то поделим обе части уравнения на** d
- **Поэтому достаточно рассмотреть случай, когда** $(a,b)=1$
- **Так как** ax **отличается от** c **на число, кратное** b**, то**

$$ax\equiv c(\mathrm{mod}\,b)$$

(без ограничения общности можно считать, что $b>0$ **)**

- **Решая это сравнение, получим** $x\equiv x_1(\mathrm{mod}\,b)$ **или**

$x=x_1+bt$ **где** $t\in Z$

Неопределённые уравнения

Диофантово уравнение первой степени с двумя неизвестными $ax+by=c$ *, где* $a,b,c\in Z$

Требуется решить это уравнение в целых числах

- **Для определения соответствующих значений y имеем уравнение $a(x_1+bt)+by=c$, откуда $y=\frac{c-ax_1}{b}-at$**

- **Причём $y_1=\frac{c-ax_1}{b}$ – целое число, оно является частным значением неизвестного y, соответствующим x_1 (получается, как и x_1, при $t=0$)**
- **А общее решение уравнения примет вид где *t* – любое целое число**

$$\begin{cases} x=x_1+bt, \\ y=y_1-at \end{cases}$$