ДАУГАВПИЛССКИЙ ПЕДАГОГИЧЕСКИЙ ИНСТИТУТ

# ВОПРОСЫ ПРЕПОДАВАНИЯ МАТЕМАТИКИ

Выпуск 2

СБОРНИК СТАТЕЙ

XXIV

ИЗДАТЕЛЬСТВО «ЗВАЙГЗНЕ»
РИГА 1975

*Ш. Х. МИХЕЛОВИЧ*

# СРАВНЕНИЯ И НЕКОТОРЫЕ ИХ ПРИМЕНЕНИЯ (НА ФАКУЛЬТАТИВНЫХ ЗАНЯТИЯХ В VIII КЛАССЕ)

## Сравнение и разбиение на классы

1. Когда мы смотрим на расписание поездов, то относительно некоторых из них находим указание: «по четным дням», а относительно некоторых других — «по нечетным дням».

Такие указания проще, чем перечисление всех чисел месяца, по которым идут поезда. Каждый хорошо знает, какие числа четные, т. е. дают при делении на два остаток нуль, и какие — нечетные, т. е. дают при делении на два остаток один.

Итак, в вопросе о сроках отправления поездов нам легче разобраться, когда указание дается в зависимости от остатка, получаемого при делении числа месяца на два, чем в зависимости от самого этого числа.

2. Аналогичное наблюдается и в других случаях, поэтому целесообразно обратить внимание на остатки, получаемые при делении целых чисел на натуральные. При этом целые числа, которые в результате их деления на одно и то же натуральное число дают один и тот же остаток, называются равноостаточными относительно этого натурального числа как модуля. Так, например, числа 47, 37 и — 23 равноостаточны по модулю 10, так как при делении на 10 они дают один и тот же остаток 7.

$$47=10\cdot4+7,\quad 37=10\cdot3+7\quad -23=10\cdot(-3)+7.$$

3. Для равноостаточных чисел $a$ и $b$ по модулю $m$ в общем случае имеем:

$$a=mq+r,\quad b=mq_1+r,\quad 0\leqslant r<m. \tag{1}$$

Такие числа великий немецкий математик К. Фр. Гаусс (1777—1855) назвал сравнимыми по модулю $m$ и ввел для них весьма удачную запись

$$a\equiv b\,(\mathrm{mod}\ m), \tag{2}$$



которая читается так: «$a$ сравнимо с $b$ по модулю $m$». Пишут также кратко: $a\equiv b(m)$, а если модуль заведомо известен, — еще более просто: $a\equiv b$. Однако следует обратить внимание на то, что числа, сравнимые по одному модулю, по другому модулю могут быть несравнимыми. Мы имеем: $47\equiv37(10)$, $47\equiv37(5)$, $47\not\equiv37(6)$, т. е. 47 не сравнимо с 37 по модулю 6.

Заметим, что целое число $a$ сравнимо со своим остатком $r$ по данному модулю $m$, т. е. $a\equiv r(m)$, напр., $47\equiv7(10)$, а целое число $a$, которое делится на модуль $m$[1], т. е. кратно $m$, сравнимо с нулем по этому модулю и наоборот.

Поэтому записи $a|m$, $a=mt$, где $t$ — некоторое целое число, и $a\equiv o(m)$ выражают одно и то же.

Имеем, напр., $15|5 \Longleftrightarrow^{2} 15=5\cdot t \Longleftrightarrow 15\equiv0(5)$.

4. Чтобы проверить сравнимость двух чисел $a$ и $b$ по модулю $m$, не обязательно устанавливать их равноостаточность по этому модулю. Из выражения (1) следует также $a-b=m(q-q_1)$, или $a-b=mt$, где $t$ — некоторое целое число, а это значит, что

$$a-b\,|\,m \tag{3}$$

или

$$a=b+mt. \tag{4}$$

Так, напр., $47\equiv37(5) \Longrightarrow 47-37|5$; $47=37+5\cdot2$. Нетрудно убедиться также в том, что соотношения (3) или (4) влекут за собой сравнение (2), так что все эти три соотношения равносильны.

5. При делении на модуль $m$ целые числа могут давать остатки $0, 1, 2, \ldots, m-1$, напр., при делении на 5 — остатки 0, 1, 2, 3, 4.

Собрав вместе все числа, которые при делении на 5 дают один и тот же остаток, т. е. числа, сравнимые между собой по данному модулю, мы соответственно получим 5 классов чисел:

| | | | | |
|---|---|---|---|---|
| . | . | . | . | . |
| . | . | . | . | . |
| . | . | . | . | . |
| −10 | −9 | −8 | −7 | −6 |
| −5 | −4 | −3 | −2 | −1 |
| 0 | 1 | 2 | 3 | 4 |
| 5 | 6 | 7 | 8 | 9 |
| 10 | 11 | 12 | 13 | 14 |
| . | . | . | . | . |
| . | . | . | . | . |
| . | . | . | . | . |

[1] Делимость $a$ на $m$ будем обозначать символом $a|m$, если $a$ на $m$ не делится, то будем писать $a \nmid m$.

[2] Знак $\Longrightarrow$ означает «влечет», а знак $\Longleftrightarrow$ — «равносильно».

Числа этих классов, т. е. расположенные в одном столбике, можно получить, если в выражениях

$$5t+0, \quad 5t+1, \quad 5t+2, \quad 5t+3, \quad 5t+4$$

вместо $t$ подставить все возможные целые значения, т. е.

$$t=0, \quad \pm 1, \quad \pm 2, \ldots .$$

6. Числа одного класса по данному модулю $m$ называются вычетами этого класса, так, напр., $-3$ и 12 являются вычетами одного класса по модулю 5. Среди вычетов класса часто обращают внимание на наименьший неотрицательный, а также на вычет, наименьший по своему абсолютному значению. Наименьший неотрицательный вычет совпадает с остатком, который получается при делении вычетов класса на модуль. В вышеупомянутом классе число 2 является одновременно вычетом наименьшим неотрицательным и наименьшим по своему абсолютному значению. В классе, которому принадлежат вычеты $-2, 3, 8, \ldots$, наименьшим неотрицательным вычетом является 3, а наименьшим по абсолютному значению $(-2)$.

Каждый вычет класса вполне определяет его, поэтому класс, которому принадлежит вычет $a$, часто обозначают символом $\bar{a} (\bmod m)$ или $\bar{a}$. Так, например, по модулю 5 класс, которому принадлежат вычеты $-7, -2, 3, 8$ и т. д., можно обозначить через $-\overline{7}$, или $-\overline{2}$, или $\overline{3}$, или $\overline{8}$ и т. д., так что $\overline{3}=\overline{8}=-\overline{2}=-\overline{7} (\bmod 5)$. Сравнимые по данному модулю числа характеризуют один и тот же класс так, как равные дроби, например, $\frac{3}{5}=\frac{6}{10}=\frac{9}{15}=\ldots$, определяют одно и то же рациональное число.

Если из каждого класса (т. е. столбика) взять по одному представителю, то полученная система чисел будет называться полной системой вычетов по данному модулю. Ее составляют, например, числа $0, 1, 2, \ldots, m-1$ или $1, 2, \ldots, m$.

### Простейшие свойства сравнений и их применение

7. Отметим некоторые свойства сравнений. В первую очередь, бросается в глаза их сходство с равенствами: а) каждое целое число сравнимо с самим собой по любому модулю, т. е. $a \equiv a (m)$ (свойство рефлексивности); б) если некоторое целое число сравнимо с другим по модулю $m$, то второе сравнимо с



первым по этому модулю, т. е. из $a \equiv b (m)$ следует $b \equiv a (m)$ (свойство симметричности); если по данному модулю целое число сравнимо с другим целым числом, последнее — с третьим, то первое число сравнимо с третьим, т. е. из $a \equiv b (m)$, $b \equiv c (m)$ вытекает $a \equiv c (m)$ (свойство переходности, или транзитивности).

Все указанные свойства вполне очевидны, так как сравнимость означает равноостаточность. Имея в виду эти свойства, говорят, что отношение сравнимости по данному модулю, так же как и отношение равенства чисел, является отношением эквивалентности. Можно указать и на ряд других отношений, выражающих отношение эквивалентности, например, равенство дробей, конгруэнтность фигур, подобие фигур.

8. Перейдем к некоторым другим важным свойствам сравнений. Оказывается, что сравнения можно, как и равенства, почленно слагать, вычитать и умножать[1], т. е.

$$a_1 \equiv b_1, \; a_2 \equiv b_2 \implies \begin{cases} a_1 \pm a_2 \equiv b_1 \pm b_2; \\ a_1 a_2 \equiv b_1 b_2. \end{cases}$$

Докажем одно из этих свойств. Пусть $a_1 \equiv b_1 (m)$, т. е. $a_1 - b_1 \mid m$. Тогда и $(a_1+a_2)-(b_1+a_2) \mid m$, или $a_1+a_2 \equiv b_1+a_2$, т. е. к обеим частям сравнения можно прибавить любое целое число. Вместе с тем можно утверждать, что слагаемое из одной части сравнения можно перенести в другую часть, изменив знак, т. е. из $a+b \equiv c \implies a \equiv c-b$.

В соответствии с доказанным из $a_2 \equiv b_2$ следует $b_1+a_2 \equiv b_1+b_2$, откуда по свойству транзитивности получаем $a_1+a_2 \equiv b_1+b_2$. Остальные свойства доказываются аналогично.

Свойства почленного сложения и умножения легко приводят к следствиям:

1) обе части сравнения можно умножать на любое целое число, т. е. $a \equiv b (m) \implies ak \equiv bk (m)$;

2) к любой части сравнения можно прибавить кратное модуля, т. е. $a \equiv b (m) \implies a \equiv b + mk (m)$;

3) обе части сравнения можно возвести в любую натуральную степень, т. е. $a \equiv b (m) \implies a^n \equiv b^n (m)$;

4) слагаемые и сомножители в сравнениях можно заменить сравнимыми числами. Если, например, $ab+cde \equiv f$, $b \equiv b_1$, $d \equiv d_1$, то и $ab_1+cd_1e \equiv f$, если $f(x)=a_0x^n+a_1x^{n-1}+\ldots+a_n$ и $x \equiv y (m)$, то $f(x) \equiv f(y) (m)$.

9. При помощи немногих сведений о сравнениях, полученных нами, можно уже решить весьма интересные задачи, например,

[1] Если не оговорено иначе, то подразумевается один и тот же модуль.

о календарных расчетах, признаках делимости и проверке арифметических действий. Рассмотрим их.

Календарные расчеты начнем со следующей задачи. Зная, что 1 января 1965 г. была пятница, найти, какой день недели был 17 мая 1965 г.

Через каждые 7 дней, считая с 1 января, повторяется пятница. Поэтому, если день 17/V 1965 г. имеет порядковый номер $S$, считая с 1 января 1965 г., то следует узнать остаток от деления $S$ на 7. Но $S$ складывается из количества дней в отдельные месяцы.

Имеем по модулю 7: в I — $31\equiv3$, в II — $28\equiv0$, в III — $31\equiv3$, в IV — $30\equiv2$, в V — $17\equiv3$, поэтому $S\equiv11$, или $S\equiv4$. Таким образом, 17/V 1965 г. — 4-й день, считая с пятницы как с первого дня, значит это был понедельник.

Назовем месячной поправкой наименьший неотрицательный вычет количества дней месяца по модулю 7.

Для невисокосного года имеем значения: для I — 3, II — 0, III — 3, IV — 2, V — 3, VI — 2, VII — 3, VIII — 3, IX — 2, X — 3, XI — 2, XII — 3.

При определении дня недели по данной дате целесообразно, в первую очередь, учесть абсолютно наименьший вычет по модулю 7 для поправок предыдущих месяцев. Будем такое число называть нарастающей месячной поправкой для соответствующего месяца и обозначать для невисокосного года через $M_н$.

| Месяц | I | II | III | IV | V | VI | VII | VIII | IX | X | XI | XII |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $M_н$ | 0 | 3 | 3 | −1 | 1 | −3 | −1 | 2 | −2 | 0 | 3 | −2 |

Понятно, что для первого и второго месяцев поправки $M_в$ в високосном году будут равны $M_н$, а для остальных месяцев — $M_в=M_н+1$.

Пользуясь табличкой для $M_н$, поставленную выше задачу можно решить быстрее, а именно: $S\equiv1+17(7)$, т. е. $S\equiv4(7)$.

Нетрудно перейти к более общей задаче: определить день недели по заданной дате, исходя из вторника — 1/I 1901 г. Для последующей даты необходимо учесть, сколько полных лет прошло с тех пор. Для каждого невисокосного года $365\equiv1(7)$, что отодвигает начало следующего года на 1 день недели; кроме того, за каждые 4 года начало года отодвигается еще на один день вследствие прошедшего високосного года; таким образом, за $n$ прошедших лет, считая с 1/I 1901 г., начало года отодвигается на $n+\left[\frac{n}{4}\right]$[1] дней. Эту поправку будем называть годичной поправкой. Теперь можем решить рассмотренную задачу, исходя из 1/I 1901 г. Имеем:



$$S\equiv1+17+64+\left[\frac{64}{4}\right] \pmod 7,$$

т. е.

$$S\equiv98, \text{ или } S\equiv0(7).$$

Поскольку 1-й день отсчета — вторник, то 0-й день — понедельник.

10. Перейдем теперь к задаче: вычислить остатки при делении на 3, 9 и 11 установить признаки делимости на эти числа. Пусть имеется число $N=56783$, его можно записать так:

$$N=3+8\cdot10+7\cdot10^2+6\cdot10^3+5\cdot10^4.$$

Но по модулю 3 $10\equiv1$, $10^k\equiv1$, поэтому $N\equiv3+8+7+6+5(3)$.

Вообще, если $N=a_0+a_1\cdot10+\ldots+a_n\cdot10^n$, то $N\equiv a_0+a_1+\ldots+a_n(3)$, т. е. остаток от деления числа на 3 равен остатку от деления на 3 суммы цифр. Вместе с тем видно, что число делится на 3 тогда и только тогда, когда сумма цифр делится на 3.

Поскольку и по модулю 9 $10\equiv1$, $10^k\equiv1$, то для 9 получается такой же признак.

По модулю 11 имеем

$$10^1\equiv-1, \quad 10^k\equiv(-1)^k,$$

поэтому

$$N\equiv a_0-a_1+a_2-+\ldots \pmod{11},$$

т. е. остаток от деления числа на 11 равен остатку от деления знакопеременной суммы цифр на 11. Число делится на 11 тогда и только тогда, когда указанная сумма делится на 11.

Заметим, что число $N$ можно также рассматривать при основании счисления 100, например, $56783=83+67\cdot100+5\cdot100^2$. Но

[1] Символом $[a]$ обозначается наибольшее целое число, не превосходящее $a$, например, $\left[5\frac{3}{4}\right]=5$.

по модулю 11 $100 \equiv 1$, $100^k \equiv 1$, поэтому $56783 \equiv 83+67+5$, а $155 \equiv 55+1 \equiv 1$.

Таким образом, остаток от деления числа $N$ на 11 равен остатку от деления на 11 суммы двузначных чисел, образованных соответствующими гранями числа $N$ при его разбиении справа налево. Число делится на 11 тогда и только тогда, когда указанная сумма делится на 11.

11. Пользуясь сравнениями, нетрудно найти условия для проверки правильности выполненных арифметических действий над целыми числами. Пусть при сложении целых $N_1$ и $N_2$ получено число $N$. Если сложение выполнено правильно, то $N_1+N_2=N$. Пусть по модулю $m$ $N_1 \equiv r_1$, $N_2 \equiv r_2$, $N \equiv r$, тогда должно также быть $r_1+r_2 \equiv r$.

Пример. При сложении получено: $375\,819+726\,345+807\,611=1\,909\,775$; проверить результат по модулю 9.

По модулю 9 абсолютно наименьшие вычеты чисел в данном соотношении равны соответственно: $-3$, 0, $-4$ и 2; условие для проверки выполняется, так как $-3+0-4 \equiv 2 \pmod 9$.

Для проверки правильности выполненных действий вычитания, умножения и деления условия получаются аналогично.

В качестве модуля для проверки целесообразно выбрать число 9, так как при этом участвуют все цифры чисел, над которыми выполняются действия. И все же проверка содержит лишь необходимое условие. На проверке не отразится, например, изменение последовательности цифр. Для повышения надежности проверки применяют дополнительно модуль 11.

## Малая теорема Ферма и теорема Эйлера

12. Аппарат сравнений станет еще намного более привлекательным, когда мы извлечем из его недр одну теорему, которую открыл величайший французский математик XVII века Пьер Ферма (1601—1665). Ее называют Малой теоремой Ферма (МТФ), и она заключается в следующем: если $p$ — простое число и $a$ на $p$ не делится, то

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

Поясним справедливость этой теоремы на числовом примере. Предварительно отметим, что на общий делитель, взаимно простой с модулем, всегда можно разделить обе части сравнения, т. е.

$$ad \equiv bd\,(m), \quad (d,\ m)=1^{[1]} \Longrightarrow a \equiv b\,(m);$$

[1] Символом $(d, m)$ обозначается наибольший общий делитель $d$ и $m$.



так как

$$(a-b)\,d \mid m, \quad (d,\ m)=1 \Longrightarrow a-b \mid m.$$

Вместо этого свойства иногда удобно пользоваться следующим равносильным свойством: если несравнимые числа умножить на число, взаимно простое с модулем, то и произведения будут несравнимыми, т. е.

$$a \not\equiv b\,(m), \quad (d,\ m)=1 \Longrightarrow ad \not\equiv bd\,(m).$$

Пусть теперь имеем некоторое простое число $p$, например 7, и пусть, кроме того, дано число $a$, например 5, которое на 7 не делится.

Составим систему чисел, умножая 5 последовательно на 1, 2, ..., 6, т. е. на все ненулевые остатки по модулю 7.

Получаем числа

$$5\cdot 1, \quad 5\cdot 2, \ldots, \quad 5\cdot 6. \tag{1}$$

По модулю 7 при этом

$$\begin{aligned} 5\cdot 1 &\equiv 5;\\ 5\cdot 2 &\equiv 3;\\ 5\cdot 3 &\equiv 1;\\ 5\cdot 4 &\equiv 6;\\ 5\cdot 5 &\equiv 4;\\ 5\cdot 6 &\equiv 2, \end{aligned} \tag{2}$$

т. е. в качестве остатков от деления чисел ряда (1) на 7 получаем те же числа 1, 2, ..., 6, только расположенные по-иному.

Это и понятно. Поскольку, например, $4 \not\equiv 3\,(7)$, а 5 — число взаимно простое с 7, то по предварительно указанному свойству $5\cdot 4 \not\equiv 5\cdot 3\,(7)$. Поэтому 6 остатков, получаемые в правой части системы (2), должны быть различными. Так как, кроме того, нулевой остаток получиться не может (поскольку $5 \nmid 7$, а также множители $1, 2, \ldots, 6 \nmid 7$), то в совокупности должны получиться все ненулевые остатки по модулю 7, т. е. числа 1, 2, ..., 6.

Перемножим все сравнения системы (2); получаем

$$5^6(1\cdot 2\cdot 3\cdot 4\cdot 5\cdot 6) \equiv (1\cdot 2\cdot 3\cdot 4\cdot 5\cdot 6) \pmod 7.$$

Так как в скобках имеем равные числа, взаимно простые с модулем, то обе части сравнения можно разделить на число в скобках, после чего получим

$$5^6 \equiv 1 \pmod 7.$$

Это сравнение и выражает для данного частного случая утверждение теоремы Ферма. В общем случае рассуждения для обоснования этой теоремы аналогичны, но мы на них останавливаться не станем.

Заметим, что $a^p \equiv a(p)$ при любом $a$ и что предложение, обратное МТФ, не имеет места.

13. Остановимся на нескольких *примерах* применения МТФ.

1) Найти остаток от деления $3^{59}$ на 17.

По модулю 17 имеем по МТФ $3^{16} \equiv 1$, так что $3^{48} \equiv 1$. Кроме того, по модулю 17: $3^3 = 27 \equiv -7$; $3^6 \equiv 49 \equiv -2$; $3^9 \equiv 14 \equiv -3$; $3^{11} \equiv -27 \equiv 7$. Итак, искомый остаток равен 7.

2) Найти остаток от деления $267^{311}$ на 37.

По модулю 37 имеем: $267 \equiv 8$, поэтому $267^{311} \equiv 8^{311}$. Но по МТФ $8^{36} \equiv 1$. Таким образом, $8^{311} = (8^{36})^8 \cdot 8^{23} \equiv 8^{23} \equiv 2^{69}$. Так как по МТФ $2^{36} \equiv 1(37)$, то остается выяснить, с чем сравнимо $2^{33}$. По модулю 37 имеем: $2^5 = 32 \equiv -5$; $2^8 \equiv -40 \equiv -3$; $2^{16} \equiv 9$; $2^{32} \equiv \equiv 81 \equiv 7$; $2^{33} \equiv 14$. Итак, искомый остаток равен 14.

3) Доказать, что $a^6 - b^6 | 7$, если $(a, 7) = 1$, $(b, 7) = 1$.

По МТФ $a^6 \equiv 1(7)$, $b^6 \equiv 1(7)$, откуда $a^6 - b^6 \equiv 0(7)$, т. е. $a^6 \equiv \equiv b^6(7)$.

4) Доказать, что для простого $p$: $(a+b)^p \equiv a^p + b^p(p)$.

По следствию из МТФ имеем: $(a+b)^p \equiv a+b(p)$; $a^p \equiv a(p)$; $b^p \equiv b(p)$, откуда и получаем $(a+b)^p \equiv a^p + b^p(p)$.

14. При помощи МТФ мы решили весьма сложные задачи. Возникает вопрос: как быть, если модуль не является простым числом? Как определить, например, остаток от деления $131^{359}$ на 242. Для такого случая петербургский академик Л. Эйлер (1707—1783) нашел важное обобщение МТФ. Чтобы его сформулировать, отметим предварительно, что количество чисел в системе

$$0, 1, 2, \dots, m-1,$$

взаимно простых с $m$, называется функцией Эйлера для $m$ и обозначается через $\varphi(m)$. Понятно, что для простого $m = p$ $\varphi(p) = p-1$. В общем случае, когда $m$ имеет разложение $m = = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, оказывается, что

$$\varphi(m) = m\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_k}\right).$$

Теперь можем сформулировать теорему Эйлера: если $a$ и $m$ числа взаимно простые, то $a^{\varphi(m)} \equiv 1(m)$. В случае простого $m$ отсюда вытекает МТФ, так как

$$\varphi(m) = \varphi(p) = p-1.$$



Поставленную выше задачу мы можем теперь решить. $131 \equiv 11(24)$, далее $\varphi(24) \equiv \varphi(2^3 \cdot 3) = 24\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right) = 8$, поэтому $131^{259} \equiv 11^{259}(24)$, а поскольку $11^8 \equiv 1(24)$, $259 = 8 \cdot 32 + 3$, то $11^{259} \equiv 11^3(24)$. Но $11^2 = 121 \equiv 1(24)$, поэтому окончательно имеем остаток 11.

## Линейные сравнения и неопределенные уравнения

15. Часто встречаются задачи, условия которых легко выразить при помощи сравнений, содержащих неизвестные.

*Пример.* На какое целое число следует умножить 3, чтобы при делении произведения на 7 в остатке получилось число 2?

Условие задачи можно записать при помощи линейного сравнения

$$3x \equiv 2\ (7). \tag{1}$$

Решение этого сравнения сводится к нахождению всех целых чисел, которые ему удовлетворяют, т. е. дают для левой части сравнения числа, сравнимые с 2 по модулю 7. Как найти такие числа? Сколько их имеется?

Заметим, что если нам удастся подобрать какое-нибудь одно число, которое сравнению (1) удовлетворяет, например $x_1$, то таким же свойством будут обладать все вычеты класса $\bar{x}_1$, так как множители, сравнимые между собой, могут заменять друг друга в сравнении. Поэтому будем искать числа, удовлетворяющие сравнению (1) только среди вычетов полной системы по модулю 7, например среди чисел

$$0, 1, 2, \dots, 6. \tag{2}$$

По модулю 7 имеем:

$$3 \cdot 0 \equiv 0;$$
$$3 \cdot 1 \equiv 3;$$
$$3 \cdot 2 \equiv 6;$$
$$3 \cdot 3 \equiv 2;$$
$$3 \cdot 4 \equiv 5;$$
$$3 \cdot 5 \equiv 1;$$
$$3 \cdot 6 \equiv 4.$$

Как видим, из вычетов системы (2) сравнению (1) удовлетворяет вычет 3, а значит и все вычеты класса $\overline{3}$.

Путем рассуждения, сходного с тем, которое применялось для обоснования МТФ, можно доказать, что и в общем случае для линейного сравнения

$$ax \equiv b(m), \text{ где } (a, m) = 1$$

среди вычетов полной системы

$$0, 1, 2, \dots, m-1$$

всегда найдется одно и только одно число $x_1$, которое ему удовлетворяет. Соответствующий класс $\bar{x}_1$ называется решением сравнения.

Указанный метод решения называется методом подбора. Вместо него можно применить метод преобразования коэффициентов, который состоит в том, что коэффициенты заменяются сравнимыми вычетами с тем, чтобы они стали по возможности меньшими по абсолютной величине и чтобы их можно было бы разделить на общий множитель. Когда таким путем мы добьемся, чтобы коэффициент у неизвестного стал равным единице, — решение найдено. В указанном выше примере достаточно к правой части прибавить модуль 7, тогда получим $3x \equiv 9(7)$, откуда $x \equiv 3(7)$.

Рассмотрим еще несколько примеров.

1) $5x \equiv 7(8)$.

Решение: $5x \equiv 7+8=15$, $x \equiv 3(8)$ или $x=3+8t$, где $t=0, \pm 1, \dots$

2) $27x \equiv 14(25)$.

Решение: $(27-25)x \equiv 14(25)$, $2x \equiv 14(25)$, $x \equiv 7(25)$.

3) $36x \equiv 23(19)$.

Решение: заменяем 36 на $(-2)$, а 23 на 4.

Получаем $-2x \equiv 4(19)$, откуда $x \equiv -2(19)$.

16. Для решения сравнения (1) можно также указать готовую формулу.

Поскольку $(a, m)=1$, имеем, согласно теореме Эйлера, $a^{\varphi(m)} \equiv 1(m)$, откуда $a(a^{\varphi(m)-1} \cdot b) \equiv b(m)$. Таким образом, решением является $x \equiv a^{\varphi(m)-1} \cdot b(m)$.

Пусть, например, имеем $3x \equiv 7(11)$.

Применяя указанную формулу, получаем $x \equiv 3^9 \cdot 7(11)$. Но надо еще потрудиться, чтобы найти вычет класса, меньший модуля. По модулю 11:

$$3^1 \equiv 3;\ 3^2 = 9 \equiv -2;\ 3^4 \equiv 4;\ 3^8 \equiv 16 \equiv 5;$$

$$3^9 \cdot 7 \equiv 28 \equiv 6, \text{ так что } x \equiv 6(11).$$



Итак, формула хороша, но при небольших модулях удобнее пользоваться методом преобразования коэффициентов.

17. Рассмотрим случай $ax \equiv b(m)$, когда $(a, m) = d > 1$, так что $a = a_1 d$, $m = m_1 d$, $(a_1, m_1) = 1$. Если при этом $b \nmid d$, то сравнение неразрешимо, так как оно равносильно уравнению $b = ax - mt = (a_1 x - m_1 t)d$, в котором правая часть делится на $d$, а левая нет.

В случае, когда $b \mid d$, т. е. $b = b_1 d$, имеем $a_1 dx \equiv b_1 d(m_1 d)$. Отсюда следует, что $a_1 x \equiv b_1(m_1)$; это сравнение разрешимо, так как $(a_1, m_1) = 1$.

Примеры:

1) $6x \equiv 5(14)$ неразрешимо, так как $(6, 14) = 2$, а $5 \nmid 2$.

2) $9x \equiv 12(21)$; здесь $(9, 21) = 3$, $12 \mid 3$. Поэтому получаем $3x \equiv 4(7)$.

Далее $3x \equiv 4+7 \cdot 2$, $3x \equiv 18$, $x \equiv 6(7)$, или $x = 6+7t$, $t=0, \pm 1, \dots$.

18. К линейному сравнению легко свести так называемое неопределенное уравнение

$$ax + by = c, \tag{1}$$

где $a, b$ и $c$ целые числа и которое надо решить в целых числах.

Заметим, что вообще под неопределенными, или диофантовыми, мы понимаем такие уравнения с целыми коэффициентами или системы таких уравнений, у которых число неизвестных больше числа уравнений. Такими уравнениями занимался еще древнегреческий математик Диофант, живший в III в. н. э., но он решал их в рациональных числах.

Рассматривая уравнение (1) по модулю $b$, получаем линейное сравнение $ax \equiv c(\mathrm{mod}\, b)$, так как $by \equiv 0(\mathrm{mod}\, b)$. После его решения и подстановки полученных значений в уравнение (1) можем также найти значение $y$.

Пример. Решить уравнение $17x - 5y = 11$.

По модулю 5 имеем $17x \equiv 11(5)$; отсюда $2x \equiv 6(5)$, $x \equiv 3(5)$ или $x = 3+5t$. Далее путем подстановки получаем: $17(3+5t) - 5y = 11$, откуда $y = 8+17t$. Итак, решениями являются пары чисел, получаемые по формулам

$$\begin{cases} x = 3+5t; \\ y = 8+17t, \quad \text{где } t = 0, \pm 1, \dots \end{cases}$$

Решений, как видим, имеется бесконечно много. Но если поставить, например, условие: $10 < x < 25$, то

$$10 < 3+5t < 25, \text{ или } 7 < 5t < 22,$$

$\frac{7}{5} < t < \frac{22}{5}$, т. е. $t$ может принять значения 2, 3, 4. Мы получим 3 решения.

19. Рассмотрим следующую занимательную задачу: найти день рождения, зная сумму $s$ произведения даты на 12 и номера месяца на 31.

Пусть, например, $s=239$. Тогда имеем

$$12x+31y=239.$$

По модулю 12 получаем сравнение $31y\equiv239(12)$, откуда $-5y\equiv-1(12)$; $-5y\equiv-25(12)$; $y\equiv5(12)$. В пределах $0<y\leqslant12$ единственное значение, удовлетворяющее этому сравнению, равно 5, оно указывает на искомый номер месяца. Соответствующее значение для $x$ равно 7, оно определяет искомую дату, так что искомый день рождения — это 7 мая.

В самом деле, пусть в общем случае имеем

$$12x+31y=s. \tag{1}$$

Согласно условию это неопределенное уравнение имеет решение $(x_1, y_1)$, где

$$0<x_1\leqslant31; \quad 0<y_1\leqslant12. \tag{2}$$

Эти значения должны удовлетворять сравнениям

$$12x\equiv s\ (31); \quad 31y\equiv s\ (12).$$

Но в указанных пределах (2) существует лишь по одному значению для $x$ и $y$, удовлетворяющих этим сравнениям. Поэтому пара чисел $(x, y)$ представляет единственное искомое решение $(x_1, y_1)$.

20. Мы рассмотрели простейшие свойства аппарата сравнений и некоторые его применения. В заключение отметим, что этот аппарат играет очень большую роль в теории чисел, он считается в этой науке универсальным методом. Сравнения проникают и в другие области знаний, так, например, на их основе создана непозиционная система счисления, которая применяется в электронных вычислительных машинах. Следует также отметить, что сравнения изучаются в одном из факультативных курсов средней школы и вызывают живой интерес учащихся.

*Э. М. ФАЛЬКЕНШТЕЙН*

# О ПРИМЕНЕНИИ ПЕРЕМЕЩЕНИЙ К РЕШЕНИЮ ГЕОМЕТРИЧЕСКИХ ЗАДАЧ В VI—VII КЛАССАХ

Изменения в содержании школьного курса геометрии существенным образом повлияли не только на содержание задач, но и на приемы их решения. Если раньше для решения почти всех геометрических задач в VI и VII классах приходилось пользоваться в том или ином виде признаками равенства треугольников, то сейчас самое широкое применение к решению задач должны найти геометрические преобразования, в частности перемещения.

Таким образом, обучение учащихся решению задач с применением геометрических преобразований становится одним из центральных вопросов методики преподавания математики в восьмилетней школе.

В настоящей статье рассматривается один из возможных путей обучения учащихся VI—VII классов решению задач с применением перемещений.

В процессе решения задач с применением перемещений можно выделить два этапа:

1) доказательство того, что фигуры, указанные в условии задачи, являются соответственными в некотором перемещении;

2) применение свойств этого перемещения.

Какую же информацию о перемещениях должен переработать и осмыслить ученик, чтобы обеспечить себе базу для успешного решения задач?

В результате работы над отдельными видами перемещений учащиеся должны усвоить, что фигура и ее образ в любом перемещении конгруэнтны, и наоборот, если две фигуры конгруэнтны, то существует перемещение, которое отображает одну из этих фигур на другую.