**Арифметика остатков**

«Остатки» играют в нашей жизни большую роль. Мы встречаемся с ними буквально на каждом шагу. Приведем несколько примеров.

1. Говоря «30 год», мы указываем век, так как 30 год может быть и в XX в., и в XIX в., и в XVIII в.; 30 – это остаток от деления полного числа лет на 100.

2. Вы взглянули на часы, которые показывают 8 ч. Но это может быть и 8 ч и 20 ч, так как часы показывают остаток от деления полного времени на 12.

3. Счетчик показывает 0314 кВт • ч. Это может быть и 0314 кВт•ч и 10314 кВт•ч и 20314 кВт•ч, так как счетчик показывает остаток от деления израсходованного числа киловатт-часов на 10 000.

Таких примеров можно привести множество. Иногда найти остаток совсем нетрудно. А как, например, найти остаток от деления числа 1996•1997•1998•1999•2000•2001 на 7? Перемножить и разделить? Представьте себе проблемы, с которыми придется столкнуться.

Эту задачу мы решим немного позже и почти устно, познакомившись с теорией «Арифметика остатков» или «Арифметика сравнений».

**Определение. Делитель в теории чисел называется модулем, а числа, дающие при делении на модуль одинаковые остатки, называются сравнимыми или равноостаточными по модулю и пишут** a≡b (mod m)**.**

Например, 8 = 7•1 + 1, 15 = 7•2 + 1. Числа 8 и 15 при делении на 7 дают одинаковые остатки, равные 1, следовательно, 8 и 15 сравнимы по модулю 7. Это записывают так: 15 $≡$ 8 (mod 7), аналогично 22 $≡$ 15 (mod 7).

В качестве модуля можно взять любое натуральное число. Например,

20 $≡$   5 (mod 3), 16$ ≡$ 4 (mod 4), 37$ ≡$ 7 (mod 10).

Вообще a$ ≡$ b (mod m), если a = mc + r, b = mc + r, где 0 m r < m.

Заметим, что если 15$ ≡$ 8 (mod 7), то (15 – 8)$ \vdots $ 7. Здесь значок $\vdots $ обозначает «кратно» или «делится на...».

Например, если 11 ≡ 5 (mod 3), то (11 – 5)$ \vdots $ 3.

Вообще, если a≡b (mod m), то a – b = (mc + r) – (md + r) = m(c – d) $\vdots $m.

Мы доказали, что если числа сравнимы по модулю m, то их разность делится на модуль m.

Верно и обратное утверждение: если разность двух чисел делится на m, по эти числа сравнимы по модулю m. Таким образом доказали теорему:

 **Теорема: Сравнение a≡b (mod m) имеет место в том и только в том случае, если разность чисел a – b делится на модуль m.**

В самом деле, если бы эти числа не были сравнимы по модулю m, то давали бы разные остатки при делении на m, но тогда их разность не могла бы делиться на m. Это свойство сравнений мы будем использовать, например, для доказательства сравнимости чисел:

10≡3 (mod 7), так как 10 – 3 = 7$\vdots $7;
21≡13 (mod 4), так как 21 – 13 = 8 $\vdots $4.

Из этого свойства вытекает способ получения сравнимых по модулю чисел: прибавить или вычесть из данного числа кратные модулю числа.

Например, 11≡8≡5≡2 (mod 3). Причем, натуральное число, меньшее модуля и сравнимое с другими числами, служит остатком от деления этих чисел на модуль. В рассмотренном примере остаток равен 2.

Приведем еще один пример: 23≡19≡15≡11≡7≡3 (mod 4).

Здесь число 3 – остаток от деления указанных чисел на 4.

***Действия над сравнениями***

1. Заметим, что

    10≡3(mod 7)
+ 12≡5(mod 7)
\_\_\_\_\_\_\_\_\_\_\_\_\_\_
   22≡8(mod 7),                              так как 22 – 8 = 14$ \vdots $ 7.

Вообще,

   a≡b(mod m), т. е. (a – b) $\vdots $ m
+ c≡d(mod m), т. е. (c – d)$ \vdots $ m
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
a + c≡b + d(mod m),                        так как (a + c) – (b + d) = (a – b) + (c – d)$ \vdots $ m.

**Мы доказали, что сравнения по одному и тому же модулю можно складывать.**

Задача 1. Найдите остаток от деления суммы  1995 + 1996 + 1997 + 1998 + 1999 на 7.

Решение.

Так как 1995 = 7•285, то 1995≡0 (mod 7), то 1995 + 1996 + 1997 + 1998 + 1999≡0 + 1 + 2 + 3 + 4 = 10≡3 (mod 7).

Остаток равен 3.

Задача 2. Найдите остаток от деления вашего года рождения, например 1988 г., на 11.

Имеем 1988 = 11•80 + 8, значит, 1998≡8 (mod 11); года рождения вашей мамы, например 1953 г., на 11. Получаем

1953 = 11•177 + 6, значит 1953≡6 (mod 11);

суммы годов рождений, вашего и маминого, на 11. Находим 1988 + 1953≡8 + 6 = 14≡3 (mod 11).

2. Заметим, что

   10≡3(mod 7)
• 12≡5(mod 7)
\_\_\_\_\_\_\_\_\_\_\_\_\_\_
120≡8(mod 7),               так как 120 – 15 = 105 $\vdots $ 7.

**Сравнения по одному и тому же модулю, можно перемножать, следовательно, и возводить в натуральную степень.**

Задача 3. Найдите остаток от деления на 7 числа 1996•1997•1998•1999•2000•2001.

Решение. Имеем   1996•1997•1998•1999•2000•2001≡1•2•3•4•5•6 = 720≡20≡6 (mod 7).

Остаток равен 7.

Часто встречаются произведения вида 1•2•3•4, 1•2•3•4•5, 1•2•3•4•5•6 и т д.

Их обозначают 1•2•3•4 = 4!, 1•2•3•4•5 = 5!. Читают: 4-факториал, 5-факториал и т. д. Вообще, 1•2•3•...•n = n! (n-факториал).

(Найдите самостоятельно значения выражений 5!, 7!.)

Заметим, что остаток от деления числа на 10 есть последняя цифра этого числа.

Пример. 21≡1 (mod 10), 134≡4 (mod 10).

Для решения ряда задач на поиски последней цифры числа полезна следующая «таблица», которую следует вывести вместе с учащимися:

|  |  |  |  |
| --- | --- | --- | --- |
| 1k≡1 (mod 10)24k≡6 (mod 10)24k+1≡2 (mod 10)24k+2≡4 (mod 10)24k+3≡8 (mod 10)5k≡5 (mod 10) | 42k≡6 (mod 10)42k+1≡4 (mod 10)34k≡1 (mod 10)34k+1≡3 (mod 10)34k+2≡9 (mod 10)34k+3≡7 (mod 10) | 6k≡6 (mod 10)92k≡1 (mod 10)74k≡1 (mod 10)74k+1≡7 (mod 10)74k+2≡9 (mod 10)74k+3≡3 (mod 10) | 92k≡ 1 (mod 10)92k+1≡9 (mod 10)84k≡6 (mod 10)84k+1≡8 (mod 10)84k+2≡4 (mod 10)84k+3≡2 (mod 10) |

  Вывод этих сравнений можно показать на примере:

7≡7 (mod 10);
72 = 49≡9 (mod 10);
73 = 72•7≡9•7 = 63≡3 (mod 10);
74 = 73•7≡3•7 = 21≡1 (mod 10).

Далее остатки будут повторяться: остаток 1 имеют все степени числа 7, показатель которых кратен 4; остаток 7 – все степени 7, показатель которых при делении на 4 дает остаток 1; остаток 9 – все степени 7, показатель которых при делении на 4 дает остаток 2; остаток 3 – все степени 7, показатель которых при делении на 4 дает остаток 3.

Задача 5. Какова последняя цифра числа137100?

Решение. Имеем:  137≡7 (mod 10), 137100≡7100 = 725•4≡1 (mod 10).

Последняя цифра равна 1.

Задача 6. Найдите последнюю цифру каждого из следующих чисел: 77, 7777.

Решение. Получаем:

77 = 74•1+3≡3 (mod 10),
7777≡777 = 74•19+1≡7 (mod 10),
Последняя цифра соответственно 3, 7.

А теперь сами попробуйте выполнить задания:

1. Найдите остаток от деления на 7суммы чисел:

а) 1995+1996+1997+1998+1999.

б) 1996+1997+1998+1999+2016+2017+2018+2019.

1. Найдите остаток от деления на 7 произведения чисел

 а) 1995•1996•1997•1998•1999.

б) 1996•1997•1998•1999•2017•2018.

1. Докажите, что n3 – n кратно 6 для любого натурального числа n.
2. Докажите, что при любом целом число делится на 6.

1. Какова последняя цифра числа137100.
2. Найдите последнюю цифру каждого из следующих чисел:

2100, 31999, 19100, 19991999, 20182018.

1. Число 7 возвели в степень 77 . Какова последняя цифра результата? От полученного числа отняли $4^{444}$. Какова последняя цифра этого результата?
2. Найдите последнюю цифру числа 19981998 + 19991999 , 20182018 + 20192019?
3. Найдите остаток от деления на 3 числа 19981998 + 19991999.