Лекция 1
Делимость целых чисел.
Теорема о делении с остатком

Теория чисел:

- ***наука о числовых системах***
- ***изучает числа с точки зрения их строения и внутренних связей, рассматривает возможности представления чисел через другие, более простые***
- ***арифметика или высшая арифметика (arithmetike от arithmos – «число», и techne – «наука»)***

Пифагорейские числа

- **Совершенные, недостаточные и избыточные числа:**
  - **недостаточные числа – те, сумма собственных делителей которых меньше самого числа (собственный делитель числа – это другое число, на которое исходное число делится нацело, включая единицу и исключая само число);**
  - **избыточные числа – те, сумма собственных делителей которых больше самого числа;**
  - **совершенные числа равны сумме всех своих собственных делителей**
- **Дружественные числа: два таких числа, каждое из которых равно сумме делителей другого. Пифагорейцам была известна лишь одна пара дружественных чисел: 220 и 284**

284=1+2+4+5+10+11+20+22+44+55+110 (сумма делителей числа 220).

220=1+2+4+71+142 (сумма делителей числа 284).

Числа близнецы

- Числа близнецы - пары простых чисел с разностью, равной двум (в пределах первой сотни):

3 и 5, 5 и 7, 11 и 13, 17 и 19, 29 и 31, 41 и 43, 59 и 61, 71 и 73

- Среди них имеются пары очень больших чисел. На 2005г. рекордсменами считались близнецы $33218925 \cdot 2^{169690} \pm 1$, найденные с помощью ЭВМ
- До сих пор неизвестно, конечно или бесконечно множество пар близнецов

- ***Учение о целых числах всегда казалось учёным неисчерпаемым полем для исследований и во все времена привлекало к себе внимание наиболее выдающихся умов***

«Эта особенность теории чисел вместе с неистощимым богатством её, которым она столь сильно превосходит другие отрасли математики, придаёт высшей арифметике неотразимое очарование, сделавшее её любимой наукой величайших математиков» (Гаусс)

Иога́нн Карл Фри́дрих Га́усс (1777 — 1855 гг.) — немецкий математик, механик, физик, астроном и геодезист

Отношение делимости. Делимость целых чисел

- В Италии существует поговорка «Трудное дело деление». Так обычно говорят, когда оказываются перед почти неразрешимой проблемой
- В Средние века людей, умевших производить деление, можно было пересчитать чуть ли не по пальцам. Их уважительно называли «магистрами деления». Они переезжали из города в город по приглашениям купцов, желавших привести в порядок свои счета

Старинная восточная притча

Давным-давно жил-был старик, который, умирая, оставил своим трём сыновьям 19 верблюдов. Он завещал старшему сыну половину, среднему – четвёртую часть, а младшему – пятую. Не сумев найти решения самостоятельно (ведь задача в «целых верблюдах» решения не имеет), братья обратились к мудрецу

Старинная восточная притча

- Нет ничего проще, - ответил им мудрец. – Возьмите моего верблюда и идите домой.

Братья дома легко разделили 20 верблюдов пополам, на 4 и на 5. Старший брат получил 10, средний – 5, а младший – 4 верблюда. При этом один верблюд остался (10+5+4=19). Раздосадованные, братья вернулись к мудрецу и пожаловались:

- О мудрец, опять мы не выполнили волю отца! Вот этот верблюд – лишний.

- Это не лишний, - сказал мудрец, - это мой верблюд. Верните его и идите домой

Определение отношения делимости

Пусть a, b $\in$ Z, b≠0. Говорят, что a делится на b, если существует c $\in$ Z, что a=b·c

- ***Обозначают:*** $a \vdots b$
- ***Говорят также: b – делитель a, b делит a (обозначают: $b \mid a$), a кратно b.***

На 0 делить нельзя

- ***Число 0 не рассматривается в качестве делителя***
- ***Действительно, если $a \neq 0$, то $a=0 \cdot q$ невозможно при любом q***
- ***Если же $a=0$, то $0=0 \cdot q$ верно при любом целом q. Однако в этом случае частное q, в отличие от остальных случаев, определяется не однозначно***
- ***Если считать, что 0 делится на 0, то это создаёт определённые неудобства***

Пример

- ***Разложим в произведение выражение a^2-a^2 двумя способами:***
- ***Имеем:***

$$a(a-a)=(a-a)(a+a)$$

- ***Разделим обе части на (а-а) и получим:***

$$a=2a$$

- ***Ещё раз разделим на а, получим, что***

$$1=2$$

Свойства делимости

1. $a \vdots a$, если a≠0

2. Если $a \vdots b$ и $b \vdots c$, то $a \vdots c$

3. Если a≠0, то $0 \vdots a$

4. Если a≠0 и $a \vdots b$, то $|a| \geq |b|$

5. Если $1 \vdots b$, то b=±1

6. Если $a \vdots b$ и $b \vdots a$, то a=±b

7. $a \vdots 1$ для любого целого a

Свойства делимости

8. Если $a \vdots c$ и $b \vdots c$, то $(a \pm b) \vdots c$
9. Если $a \vdots c$ и b ϵ Z, то $ab \vdots c$
10. Если $a_1, a_2, \ldots, a_n \vdots c$ и $b_1, b_2, \ldots, b_n \in Z$, то $(a_1b_1 + a_2b_2 + \ldots + a_nb_n) \vdots c$
11. Если $(a+b) \vdots c$ и $b \vdots c$, то $a \vdots c$
12. Если $(a+b) \vdots c$ и b не $\vdots c$, то a не $\vdots c$
13. Если $a \vdots c$ и $b \vdots d$, то $(ab) \vdots cd$
14. Если $a \vdots c$ и $b \epsilon N$, то $(ab) \vdots cb$
15. Если $(ab) \vdots cb$, то $a \vdots c$
16. Если $a \vdots b$, то $\pm a \vdots (\pm b)$

Теорема о делении с остатком

Для любого целого числа a и любого целого $b \neq 0$ существуют и единственные целые числа q и r, такие, что

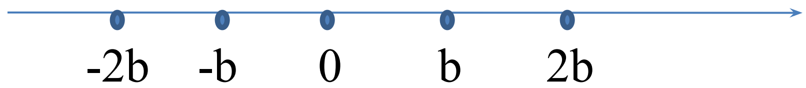
$$a = bq + r, \text{ где } 0 \leq r < |b|$$

Число q называют неполным частным,

r – остатком

Доказательство

1) b>0. Рассмотрим числовую прямую и разобьем её на отрезки длины b точками 0, ±b, ±2b, ±3b, …



Очевидно, что где бы ни было расположено число a, оно обязательно попадёт в один из полуинтервалов

[bq, b(q+1)), где q – целое, так как числовая прямая – объединение всех таких полуинтервалов. То есть найдётся целое q, что $bq \le a \le b(q+1)$. К каждой части неравенства прибавим –bq, получим $0 \le a-bq < b$

Обозначим a-bq=r. Тогда a=bq+r, $0 \le r < b = |b|$

2) b<0. Тогда –b > 0 и по доказанному для a и –b существуют целые q и r, что a=(-b)q+r, $0 \le r < |-b|$. Откуда получаем:

a=b(-q)+r, где $0 \le r < |b|$. Существование q и r доказано

Доказательство

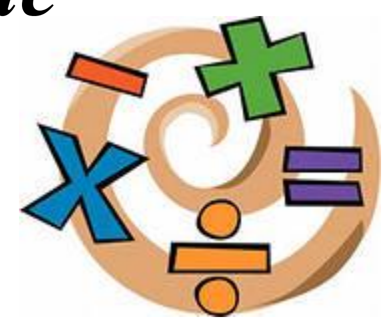
Докажем единственность.

- ***Пусть** $a = bq + r$, $0 \le r < |b|$, **и** $a = bq_1 + r_1$, $0 \le r_1 < |b|$*
- ***Имеем:** $bq + r = bq_1 + r_1$, $b(q - q_1) = r_1 - r$*

□ ***Если** $q = q_1$, **то** $r_1 = r$* $\vdots\, b$

□ ***Если же** $q \ne q_1$, **то** $(r_1 - r)$ **и, следовательно,** $|r_1 - r| \ge |b|$ **(свойство делимости 5)***

- ***Однако** $|r_1 - r| < |b|$ **- противоречие***
- ***Следовательно,** $q = q_1$, $r_1 = r$*



Ребус