<u>Лекция 2</u> . НАЧАЛЬНЫЕ СВЕДЕНИЯ ИЗ ТЕОРИИ ЦЕЛЫХ ЧИСЕЛ
(применительно к теории помехоустойчивых кодов)

1. Классификация чисел: целые, дробные, положительные, отрицательные, натуральный ряд целых чисел, рациональные числа, иррациональные, мнимые.

2. Системы счисления. Основание системы счисления. Примеры: десятичная (p=10), двоичная (p =2), шестнадцатеричная (p =16)

3. Операции над числами: сложение, вычитание, умножение, деление.

4. Кратные числа: *Число a кратно b, если $a=bq$ (по умножению) и $a/b=q$ (по делению).* Деление часто обозначают $b|a$ (b делит a).

5. Число *a* не кратно *b*, *если $a=bq+r$ (по умножению) и $a/b=q+r/b$ (по делению), где r остаток ($0<r<b$).*

6. Общий делитель: *всякое целое число d , являющееся одновременно делителем целых чисел (a,b,c,…), называется общим делителем этих чисел.*
Наибольший общий делитель (НОД) – *это наибольший из всех общих делителей чисел (a,b,c,…), который часто обозначается как НОД(a,b,c,…).*

Свойства общих делителей:

***Свойство 1**. Если число a кратно числу b и b < a, то совокупность общих делителей чисел a и b совпадает с совокупностью делителей b. Но так как b|a , то НОД(a,b)=b.*

***Свойство 2**. Если число a не является кратным числу b и b < a, т. е. a = bq+r, 1≤ r < b, то НОД(a,b) находится по алгоритму Евклида.*

Алгоритм Евклида.

Решение является итеративной процедурой:

1-ая итерация: $a = bq_1 + r_1; \quad 0 < r_1 < b;$

2-ая итерация: $b = r_1 q_2 + r_2; \quad 0 < r_2 < r_1;$

3-ья итерация: $r_1 = r_2 q_3 + r_3; \quad 0 < r_3 < r_2;$

……. .....

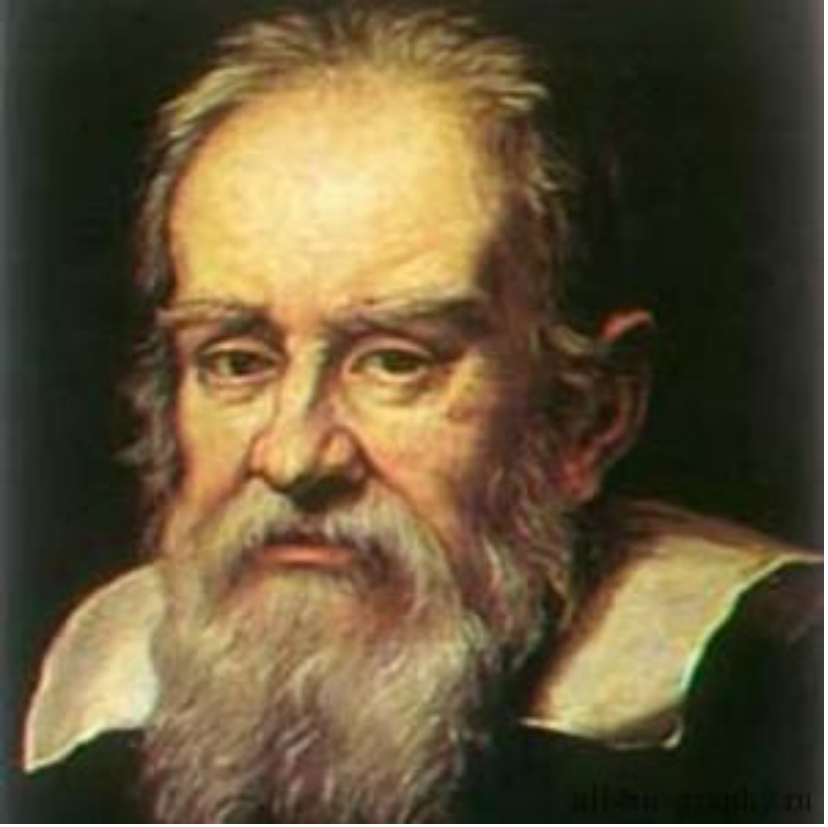
n-ая итерация: $r_{n-2} = r_{n-1} q_n + r_n; \quad 0 < r_n < r_{n-1};$

(n+1)-ая итерация: $r_{n-1} = r_n q_{n+1}; \quad r_{n+1} = 0.$

СТОП на $(n+1)$-ой итерации, когда остаток r_{n+1} стал равным 0.

Тогда предыдущий остаток r_n и будет наибольшим общим делителем

$$НОД(a,b) = r_n$$



Евклид родился около 330 г. до н.э., предположительно, в г. Александрия. Некоторые арабские авторы полагают, что он происходил из богатой семьи из Нократа. Есть версия, что Евклид мог родиться в Тире, а всю свою дальнейшую жизнь провести в Дамаске. Согласно некоторым документам, Евклид учился в древней школе Платона в Афинах, что было под силу только состоятельным людям. Уже после этого он переедет в г. Александрия в Египте, где и положит начало разделу математики, ныне известному как «геометрия».

Евклида обоснованно считают «отцом геометрии». После переезда в Александрию, Евклид, как и многие учёные того времени, благоразумно проводит большую часть времени в Александрийской библиотеке. Этот музей, посвящённый литературе, искусству и наукам, был основан ещё Птолемеем. Здесь Евклид начинает объединять геометрические принципы, арифметические теории и иррациональные числа в единую науку геометрию. Он продолжает доказывать свои теоремы и сводит их в колоссальный труд «Начала». За всё время своей малоисследованной научной деятельности, учёный закончил 13 изданий «Начал», охватывающих широкий спектр вопросов, начиная с аксиом и утверждений и заканчивая стереометрией и теорией алгоритмов.

***Свойство 3**. Для двух целых am и bm НОД(am,bm) = НОД(a,b)·m.*

***Свойство 4**. Если число d - общий делитель чисел a и b , то*

$$НОД(\frac{a}{d},\frac{b}{d}) = \frac{НОД(a,b)}{d}.$$

***Свойство 5**. Натуральное число p называется простым, если оно делится только на 1 и на само себя.*

***Свойство 6**. Если НОД(a,b)=1, то такие два числа называются взаимно простыми.*

***Свойство 7**. Если каждое из чисел $a_1, a_2, ..., a_m$ является взаимно простым с каждым из чисел $b_1, b_2, ..., b_n$, то и произведение чисел $a_1, a_2, ..., a_m$ будет взаимно простым с произведением чисел $b_1, b_2, ..., b_n$*

***Свойство 8**. Отыскание НОД более, чем двух целых чисел $a_1, a_2, ..., a_m$ сводится к пошаговой процедуре нахождения НОД двух чисел:*

$$\left.\begin{array}{l} НОД(a_1, a_2) = d_2; \\ НОД(d_2, a_3) = d_3; \\ НОД(d_3, a_4) = d_4; \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ НОД(d_{n-1}, a_n) = d_n; \end{array}\right\}$$

Т.е. $НОД(a_1, a_2, ..., a_m) = d_n.$

7. Наименьшее общее кратное (НОК) – ***это наименьшее число, кратное всем заданным числам.***

Свойства НОК:

<u>Свойство 1.</u> НОК двух чисел a и b равно их произведению, делённому на их НОД.

<u>Свойство 2.</u> НОК двух простых чисел a и b (т.е. НОД(a,b)=1) равно их произведению: НОК(a,b)=a·b.

8. Каноническое разложение числа на простые множители. ***Всякое целое число, большее «1», разлагается на произведение простых сомножителей единственным способом с точностью до перестановки:***

$$a = p_{i1} p_{i2} \cdots p_{in}.$$

При этом некоторые из простых сомножителей могут повторяться. Обозначая буквами $p_{j1}, p_{j2}, \ldots, p_{jk}$ ***различные из простых сомножителей и буквами*** $m_1, m_2, \ldots, m_k$ ***кратности их вхождения в разложение числа a, получим разложение вида*** $a = p_{j1}^{m_1} \cdot p_{j2}^{m_2} \cdots p_{jk}^{m_k}$,

которое называется каноническим разложением числа a на сомножители простых чисел $p_{j1}, p_{j2}, \ldots, p_{jk}$.

9. ОСНОВНЫЕ ФУНКЦИИ ТЕОРИИ ЧИСЕЛ

9.1. Целая часть числа *X* – *это наибольшее целое, не превосходящее X;* $\lfloor X \rfloor$

9.2. Дробная часть числа X – $]X[= X - \lfloor X \rfloor .$

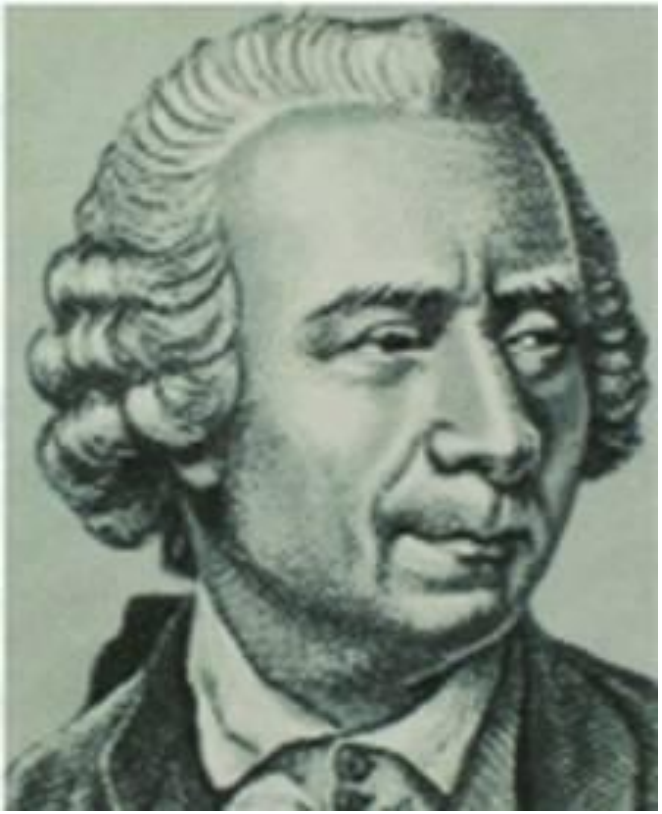
9.3. Функция Эйлера числа *a* – φ(*a*), *определяется для всех целых и положительных чисел a и представляет собой количество чисел ряда 1,2,3,…,(a-1) взаимно простых с a, включая «1».*

- ***Функция Эйлера от простого числа p равна* φ(*p*)=*p*-1.**

- ***Если число a представить в каноническом разложении*** $a = p_{j1}^{m_1} \cdot p_{j2}^{m_2} \cdots p_{jk}^{m_k}$ ***, то функция Эйлера от «a» определяется выражением***

$$\varphi(a) = \prod_{i=1}^{k} p_i^{m_i - 1}(p_i - 1); \quad p_i > 1.$$

- ***Функция Эйлера мультипликативная: если число a равно произведению двух взаимно простых чисел b и c таких, что НОД(b,c)=1, то выполняется равенство:*** $\varphi(a) = \varphi(b \cdot c) = \varphi(b) \cdot \varphi(c).$



Леонард Эйлер () — математик, механик, физик и астроном. По происхождению швейцарец.
В 1726 году Леонард Эйлер был приглашен в Петербургскую АН и переехал в 1727 в Россию. Был адъюнктом (1726), а в 1731-41 и с 1766 академиком Петербургской АН (в 1742-66 иностранный почетный член). В 1741-66 работал в Берлине, член Берлинской АН

Л. Эйлер — ученый необычайной широты интересов и творческой продуктивности. Автор свыше 800 работ по математическому анализу, дифференциальной геометрии, теории чисел, приближенным вычислениям, небесной механике, математической физике, оптике, баллистике, кораблестроению, теории музыки и других, оказавших значительное влияние на развитие науки. За время существования Академии наук в России, считается одним из самых знаменитых ее членов.

10. СРАВНЕНИЯ И ИХ СВОЙСТВА

Каждому целому числу «a» отвечает определённый остаток r при делении его на число m:

$$\frac{a}{m} = q + \frac{r}{m} \qquad \text{или} \qquad a = mq + r, \qquad \text{где} \quad q - \text{частное}.$$

Это означает, что "a" сравнимо с r по модулю m. $\Rightarrow a \equiv r (\mathrm{mod}\, m).$

Свойство 1. Если $a \equiv r \ (\mathrm{mod} m)$ и $b \equiv r \ (\mathrm{mod} m)$, $a \neq b$, **то такие числа называются равноостаточными по модулю *m* или сравнимыми по модулю *m***

$$a \equiv b (\mathrm{mod} m).$$

Свойство 2. **Два числа *a* и *b*, сравнимые с третьим числом *c* по модулю *m*, также сравнимы между собой по модулю *m*:**

$a \equiv c \ (\mathrm{mod} m)$ и $b \equiv c \ (\mathrm{mod} m)$, тогда $a \equiv b \ (\mathrm{mod} m)$.

***Свойство* 3**. **Слагаемое, стоящее в какой-либо части сравнения, можно переносить в другую часть с изменением знака на обратный:**

Если $(a + c) \equiv b \ (\mathrm{mod} m)$, то **$a \equiv (b - c) \ (\mathrm{mod} m)$.**

***Свойство* 4**. **К любой части сравнения можно добавить любые числа, кратные модулю *m*:**

$$a \equiv b (\mathrm{mod}\, m) \Rightarrow a + mt_1 \equiv b + mt_2 (\mathrm{mod}\, m), \quad t_1, t_2 \geq 1.$$

***Свойство* 5. Отрицательное число (-*a*) сравнимо по mod*m* с числами**

(-*a*) + *mt*; *t* – целое число.

***Свойство* 6. Аддитивность сравнений – сравнения по mod*m* можно почленно складывать**

$$a_1 \equiv b_1 (\mathrm{mod}\, m);\quad a_2 \equiv b_2 (\mathrm{mod}\, m) \quad \Rightarrow (a_1 + a_2) \equiv (b_1 + b_2) (\mathrm{mod}\, m).$$

***Свойство 7*. Мультипликативность сравнений – сравнения по mod*m* можно почленно перемножать**

$$a_1 \equiv b_1 (\mathrm{mod}\, m);\quad a_2 \equiv b_2 (\mathrm{mod}\, m) \quad \Rightarrow (a_1 \cdot a_2) \equiv (b_1 \cdot b_2) (\mathrm{mod}\, m).$$

***Свойство 8*. Обе части сравнения можно возвести в одну и ту же степень:**

$$a \equiv b (\mathrm{mod}\, m) \Rightarrow a^k \equiv b^k (\mathrm{mod}\, m).$$

***Свойство 9*. Обе части сравнения можно умножать на одно и то же целое:**

$$a \equiv b (\mathrm{mod}\, m) \Rightarrow a \cdot c \equiv b \cdot c (\mathrm{mod}\, m)$$

11. ВЫЧЕТЫ ПО mod*m*

Все числа, сравнимые по модулю m, образуют класс чисел по модулю m. Всем числам одного и того же класса отвечает один и тот же остаток r (0≤ r < m). Так как r принимает значения от 0 до (m-1) включительно, то имеется m различных классов чисел по* mod*m.

Любое число класса r по модулю m является вычетом по* mod*m.

Вычет, равный самому остатку r, называется наименьшим неотрицательным вычетом или образующим класса «r» по* mod*m.

Свойство* 1. *Полная система вычетов – это совокупность вычетов, взятых по одному из каждого класса. Чаще всего в качестве полной системы вычетов берут наименьшие неотрицательные вычеты или образующие классов* 0,1,2,…,(m-1) *по модулю m.

Свойство* 2. *Приведенная система вычетов по* mod*m– это совокупность вычетов среди наименьших неотрицательных вычетов (или образующих классов) по* mod*m, взаимно простых с m. Число элементов в такой приведённой системе вычетов равно функции Эйлера* φ(m), *а значения элементов в этой системе – это числа меньшие m и взаимно простые с ним.

Свойство* 3.** ***Для приведённой системы вычетов справедливы следующие теоремы:

<u>Теорема Эйлера</u>: При взаимно простых *a* и *m*, *m* > 1, НОД(*a*,*m*)=1, выполняется сравнение $a^{\varphi(m)} \equiv 1 (\mathrm{mod}\, m).$

<u>Теорема Ферма</u>: При простом *p* и *a* взаимно простом с *p* выполняется сравнение $a^{p-1} \equiv 1 (\mathrm{mod}\, p).$

12. ПОКАЗАТЕЛИ ЭЛЕМЕНТА (ЧИСЛА)

Для любого целого числа *a*, взаимно простого с числом *m*, при возведении данного числа *a* в последовательные степени, начиная с 1, всегда найдётся такое наименьшее положительное число *n* (*n* > 0), для которого выполняется сравнение $a^n \equiv 1 (\mathrm{mod}\, m).$

Показатель элемента. **Минимальное целое число *n* > 0, для которого выполняется указанное выше сравнение, называется показателем, которому принадлежит число *a* по mod*m*.**