Основы теории чисел
Теория сравнений

История теории чисел

- В истоках теории чисел как научной дисциплины выделяются исследования Евклида (3 век до н. э.), Диофанта (3 век н. э.), Ферма (1601-1665), Эйлера (1707-1783), сохранившиеся в письменном виде.
- Исторические источники подтверждают, что создателем теории чисел является Эйлер. При этом следует отметить, что несколько теорем из теории чисел (как правило без доказательств) были сформулированы до Эйлера.

- Каждое натуральное число, большее единицы, делится по крайней мере на два числа: на 1 и на само себя. Если число не имеет делителей, кроме самого себя и единицы, то оно называется простым, а если у числа есть еще делители, то составным. Единица же не считается ни простым числом, ни составным. Например, числа 7, 29— простые; числа 9, 15 — составные (9 делится на 3, 15 делится на 3 и на 5).

- Не о всяком числе можно сразу сказать, простое оно или составное. Если число меньше ста, то, скорее всего мы сразу сможем ответить на этот вопрос. Однако с большими числами дело сложнее.
- Бывает, что проверка на простоту производиться гораздо дольше, а для работы с большими целыми числами требуются даже специальные компьютерные программы.
- Поиск больших простых чисел имеет важное значение для математики и не только. Например, в криптографии большие простые числа используются в алгоритмах шифрования с открытым ключом. Для обеспечения надежности шифрования там используются простые числа длиной до 1024 бит.

- Перемножить два числа сравнительно нетрудно, особенно если у нас есть калькулятор, а числа не слишком велики. Существует и обратная задача – **задача факторизации** – нахождение двух или более чисел, дающих при перемножении заданное число. Эта задача гораздо труднее, чем перемножение чисел, и любому, кто пытался ее решить, об этом известно.
- Например, если от нас требуется умножить 67 на 113, то результат, 7571, будет получен, наверно, меньше чем за минуту. Если же от нас требуется найти два числа, произведение которых равно 7571, то, скорее всего, это займет у нас гораздо больше времени.

Основная теорема арифметики

- Любое составное число можно составить из некоторого количества простых с помощью умножения. Например, составное число 2009 можно получить так:

  2009 = 7 * 7 * 41

- В математике рассматривается так называемая основная теорема арифметики, которая утверждает, что **любое натуральное число (n>1) либо само является простым, либо может быть разложено на произведение простых делителей, причем единственным способом.**
- Воспользовавшись обозначением степени, разложение числа 2009 на простые множители можно записать так: 2009 = 72 * 41
- Разложение на множители называется **каноническим**, если все множители являются простыми и записаны в порядке возрастания.

Взаимно простые числа и функция Эйлера

- Два числа называются взаимно простыми, если они не имеют ни одного общего делителя кроме единицы.
- Например, числа 11 и 12 взаимно просты (у них нет общих делителей кроме единицы), числа 30 и 35— нет (у них есть общий делитель 5).
- Исследованием закономерностей, связанных с целыми числами, долго занимался швейцарский математик Леонард Эйлер. Одним из вопросов, которым он интересовался, был следующий: сколько существует натуральных чисел, не превосходящих n и взаимно простых с n?
- Ответ на этот вопрос был получен Эйлером в 1763 году и этот ответ связан с каноническим разложением числа n на простые множители.

Число натуральных чисел, не превосходящих n и взаимно простых с n, называется функцией Эйлера и обозначается $\phi(n)$.

$$n = p_1^{a1} \times p_2^{a2} \times \cdots \times p_n^{a_n}$$

$$\varphi(n) = n \times \left(1 - \frac{1}{p_1}\right) \times \left(1 - \frac{1}{p_2}\right) \times \cdots \times \left(1 - \frac{1}{p_n}\right)$$

Пример

- Например, найдем количество натуральных чисел, не превосходящих 12 и взаимно простых с 12. Из ряда натуральных чисел 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11 взаимно простыми (не имеющими общих делителей) с 12 будут только числа 1, 5, 7, 11. Их количество равно четырем.

- Воспользуемся функцией Эйлера и тоже получим 4.

Для этого вначале запишем каноническое разложение числа 12: **$12 = 2^2 * 3$.**

$$\varphi(12) = 12 \times \left(1 - \frac{1}{2}\right) \times \left(1 - \frac{1}{3}\right) = 4 \times 3 \times \frac{1}{2}\frac{2}{3} = 4$$

- Формулу Эйлера удобно использовать для больших n, если известно разложение числа n на простые множители.
- Для криптографии формула Эйлера важна тем, что она позволяет легко получить число для простых и некоторых других чисел.
- Эйлер был одним из первых, кто использовал и даже усовершенствовал алгоритм Евклида в арифметической форме.

Нахождение НОД по алгоритму Евклида

- **Алгоритм Евклида** – это алгоритм нахождения наибольшего общего делителя (НОД) пары целых чисел.
- **Наибольший общий делитель (НОД)** – это число, которое делит без остатка два числа и делится само без остатка на любой другой делитель данных двух чисел. Проще говоря, это самое большое число, на которое можно без остатка разделить два числа, для которых ищется НОД.

Описание алгоритма нахождения НОД делением

1. Большее число делим на меньшее.

2. Если делится без остатка, то меньшее число и есть НОД (выход из цикла).

3. Если есть остаток, то большее число заменяем на остаток от деления.

4. Переходим к пункту 1.

Пример 1: Найти НОД для 30 и 18.

30/18 = 1 (остаток 12)

18/12 = 1 (остаток 6)

12/6 = 2 (остаток 0).

НОД (30, 18) = 6

Нахождение НОД с помощью разложения чисел на простые множители

- Наибольший общий делитель может быть найден по ***разложениям чисел на простые множители***.

Сформулируем правило:

- НОД двух целых положительных чисел a и b равен произведению всех общих простых множителей, находящихся в разложениях чисел a и b на простые множители.

Найдите наибольший общий делитель чисел 72 и 96

Решение.

Разложим на простые множители числа 72 и 96:

$72=2\cdot2\cdot2\cdot3\cdot3$

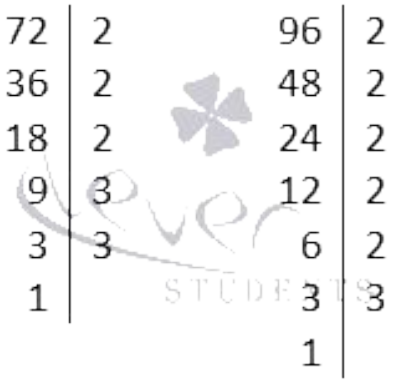
$96=2\cdot2\cdot2\cdot2\cdot2\cdot3$

Общими простыми множителями являются 2, 2, 2 и 3.

Таким образом, НОД(72, 96)$=2\cdot2\cdot2\cdot3=24$.

Ответ:

НОД(72, 96)=24.



Нахождение НОД трех и большего количества чисел

Нахождение наибольшего общего делителя трех и большего количества чисел может быть сведено к последовательному нахождению НОД двух чисел.

Наибольший общий делитель нескольких чисел *a1, a2, ..., ak* равен числу *dk*, которое находится при последовательном вычислении *НОД(a1, a2)=d2*, *НОД(d2, a3)=d3*, *НОД(d3, a4)=d4*, …, *НОД(dk-1, ak)=dk.*

Найти НОД (*78, 294, 570* и *36)*

1) По алгоритму Евклида определим наибольший общий делитель *d2* двух первых чисел *78* и *294*.

При делении получаем равенства $294=78\cdot3+60$; $78=60\cdot1+18$; $60=18\cdot3+6$ и $18=6\cdot3$.

Таким образом, $d2=НОД(78, 294)=6$.

2) Вычислим $d3=НОД(d2, a3)=НОД(6, 570)$. Т. к.$570=6\cdot95$, значит, $d3=НОД(6, 570)=6$.

3) Вычислим $d4=НОД(d3, a4)=НОД(6, 36)=6$.

Таким образом, наибольший общий делитель четырех данных чисел равен $d4=6$.

$НОД(78, 294, 570, 36)=6$.

Нахождение наименьшего общего кратного (НОК) данных чисел

- Наименьшим общим кратным данных натуральных чисел называют наименьшее натуральное число, кратное каждому из данных чисел.

Пример.

НОК(24, 42)=168. Это самое маленькое число, которое делится и на 24, и на 42.

Нахождение наименьшего общего кратного

Для нахождения НОК нескольких данных натуральных чисел надо:

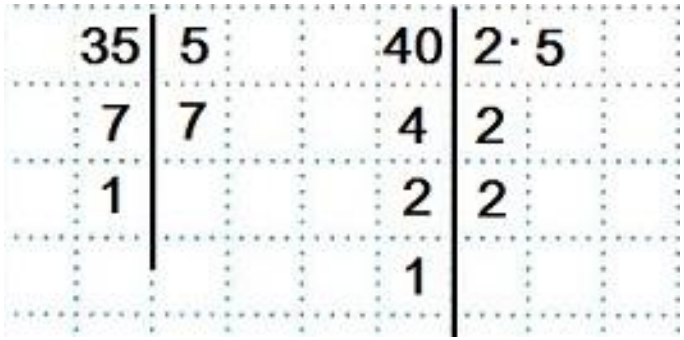
1) разложить каждое из данных чисел на простые множители;

2) выписать разложение большего из чисел и умножить его на недостающие множители из разложений других чисел.

Наименьшее кратное двух взаимно простых чисел равно произведению этих чисел.

Найти НОК(35; 40)

Разложим числа 35 и 40 на простые множители



$35=5\cdot7$, $40=2\cdot2\cdot2\cdot5$ или $40=2^3\cdot5$

Берем разложение большего числа 40 и дополняем его недостающими множителями.

НОК(35; 40)$=2^3\cdot5\cdot7=40\cdot7=280$.

Ответ: НОК(35; 40)=280.

Найти НОК (75; 120; 150)

Разложим числа 75, 120 и 150 на простые множители.

$75=3\cdot5^2$, $120=2^3\cdot3\cdot5$, $150=2\cdot3\cdot5^2$

Возьмем разложение большего числа 150 и дополним его двумя «двойками», так как в разложении числа 120 имеется три «двойки», а в разложении числа 150 – только одна.

НОК(75; 120; 50)$=2\cdot3\cdot5^2\cdot2\cdot2=150\cdot4=600$.

Ответ: НОК(75; 120; 150)=600.

Теория сравнений

Каждому целому числу отвечает определённый остаток от деления его на m;

если двум целым a и b отвечает один и тот же остаток m, то они называются **равноостаточными** по модулю m или **сравнимыми по модулю** m.

Сравнимость чисел a и b по модулю m записывается так: $a \equiv b \pmod{m}$,

что читается: a сравнимо с b по модулю m.

- Сравнения обнаруживают полезные для математиков и криптографов свойства, во многом похожие на свойства равенств.
- Эти свойства позволяют существенно упрощать арифметические вычисления.
- Так, например, свойства сравнений полезны при расчетах в алгоритмах шифрования с открытым ключом.

Свойства сравнений

1. Если a - b делится на m, то $a \equiv b(mod\ m).$

Например, $15 \equiv 1(mod\ 7),$

так как 15 -1 =14, а 14 кратно 7.

2. Если $a \equiv b(mod\ m) \quad c \equiv d(mod\ m)$

то $a + c \equiv b + d(mod\ m)$

$ac \equiv bd(mod\ m)$

Например, $13 \equiv 5(mod\ 8) \qquad 11 \equiv 3(mod\ 8),$

то $13 + 11 \equiv 5 + 3 \equiv 0(mod\ m),$

$13 * 11 \equiv 5 * 3 \equiv 7(mod\ 8).$

Свойства сравнений

3. Если $a \equiv b(mod\ m), \quad$ то $a^k \equiv b^k(mod\ m), k \subset N.$

4. Если, $ac \equiv bc(mod\ m)$ то с взаимно простое с m.

Например $1200 \equiv 45(mod\ 7),$

Тогда $1200 = 15 * 80$ и $45 = 15 * 3,$ то

$80 \equiv 3(mod\ 7)$

Малая теорема Ферма

В основе алгоритма шифрования по системе RSA лежит теорема, сформулированная в начале семнадцатого столетия без доказательства французским математиком Пьером Ферма (Pierre Fermat). Её часто называют "Малой теоремой Ферма".

Если p - простое число, а m – любое число, которое не делится на p, то $m^{p-1} \equiv 1 (mod\ p),$

то есть число m^{p-1} при делении на p дает остаток 1.