[1) Классическое определение вероятности 3](#_Toc92388292)

[2) Случайные события, действия над случайными событиями 4](#_Toc92388293)

[3) Теорема сложения и умножения вероятностей. Совместные и несовместные события. Зависимые и независимые 4](#_Toc92388294)

[4) Формула полной вероятности. Примеры 6](#_Toc92388295)

[5) Схема Бернулли. Предельные теоремы в схеме Бернулли 7](#_Toc92388296)

[6) Определение случайной величины. Функция распределения СВ и ее свойства 8](#_Toc92388297)

[7) Дискретные СВ, способы их задания 9](#_Toc92388298)

[8) Непрерывные СВ, способы их задания 10](#_Toc92388299)

[9) Плотность распределения СВ и ее свойства 10](#_Toc92388300)

[10) Математическое ожидание СВ, формулы для вычисления 12](#_Toc92388301)

[11) Дисперсия СВ и ее свойства. Среднеквадратическое отклонение 13](#_Toc92388302)

[12) Биномиальное распределение 14](#_Toc92388303)

[13) Распределение Пуассона 14](#_Toc92388304)

[14) Геометрическое распределение 15](#_Toc92388305)

[15) Равномерное распределение 17](#_Toc92388306)

[16) Показательное распределение 17](#_Toc92388307)

[17) Нормальный закон распределения. Правило трех сигм 19](#_Toc92388308)

[18) Понятие о двумерной СВ. Функция распределения двумерной СВ и ее свойства 19](#_Toc92388309)

[19) Распределение непрерывной двумерной СВ. Совместная плотность распределения. Распределение СВ по 20](#_Toc92388310)

[20) Условие независимости и некоррелируемости СВ "пси" и "эта", связь между ними 21](#_Toc92388311)

[21) Числовые характеристики двумерных СВ "пси" и "эта", математитческое ожидание, дисперсия, сигма, ковариация СВ 22](#_Toc92388312)

[22) Коэффициент корелляции СВ и его свойства 23](#_Toc92388313)

[23) Основные задачи математической статистики. Выборка, вариационный ряд 24](#_Toc92388314)

[24) Эмпирическая функция распределения и ее свойства 25](#_Toc92388315)

[25) Точечная оценка параметров распределения, их свойств (4 штуки) 26](#_Toc92388316)

[26) Точечная оценка математического ожидания, его свойства 27](#_Toc92388317)

[27) Точечная оценка дисперсии, формула ее вычисления, свойства 28](#_Toc92388318)

[28) Интервальные оценки доверительной вероятности 30](#_Toc92388319)

[29) Доверительный интервал для неизвестного математического ожидания нормального распределения СВ при известной дисперсии 31](#_Toc92388320)

[30) Доверительный интервал для неизвестного математического ожидания нормального распределения СВ при НЕизвестной дисперсии 32](#_Toc92388321)

[31) Проверка статистических гипотез 33](#_Toc92388322)

[32) Критерий Пирсона 33](#_Toc92388323)

[33) Целые числа. Свойства делимости. Простые числа и их свойства 34](#_Toc92388324)

[34) Критерий взаимной простоты чисел. Основная теорема арифметики 35](#_Toc92388325)

[35) НОК и НОД, алгоритм Евклида 36](#_Toc92388326)

[36) Соотношение Безу 37](#_Toc92388327)

[37) Диафантовые линейные уравнения 38](#_Toc92388328)

[38) Сравнение целых чисел. Свойства сравнений 39](#_Toc92388329)

[39) Множество классов вычетов 28](#_Toc92388330)

[40) Функция Эйлера. Теорема Эйлера. Малая теорема Ферма 41](#_Toc92388331)

[41) Решение линейных сравнений 42](#_Toc92388332)

[42) Алгебраические операции. Понятие группы и подгруппы, примеры 43](#_Toc92388333)

[43) Порядок элементов в группе. Циклические группы 44](#_Toc92388334)

[44) Смежные классы. Теорема Логранжа 45](#_Toc92388335)

[45) Нормальные подгруппы. Фактор группы 46](#_Toc92388336)

[46) Понятие кольца и подкольца, примеры 47](#_Toc92388337)

[47) Мультпликативная группа кольца, делители нуля 48](#_Toc92388338)

[48) Идеалы колец. Кольцо полиномов 49](#_Toc92388339)

[49) Теорема Безу и корни многочленов 51](#_Toc92388340)

[50) Поле. Примеры полей 51](#_Toc92388341)

[51) Характеристика поля. Примеры конечных полей. Поля Галуа 54](#_Toc92388342)

# **1) Классическое определение вероятности**

Теория вероятности изучает неслучайные закономерности массовых случайных явлений. Причем, рассматривает те явления, которые могут быть неоднократно повторены в одинаковых условиях.

Набор условий называется **случайным экспериментом.**

Результаты случайного эксперимента называют **случайным событием или событием** ( обозн.: А, В, С).

**Случайное событие** – это то что может произойти или не произойти в результате ряда экспериментов.

Множество всевозможных итогов случайного эксперимента называется **вероятностным пространством** ( + Ω={ ω1 ,ω2 ,…ωn})

Элементарное событие называется благоприятствующим событию A, если его появление влечет за собой появление события A.

**Классическое определение вероятности**

Вероятностью P(A) случайного события A называется отношение числа m благоприятствующих ему элементарных событий к их общему числу n.

**Основные свойства вероятности**

1. Вероятность случайного события A есть неотрицательное число, заключенное между нулем и единицей, т. е. 0 ≤ P(A) ≤ 1.

2. Вероятность достоверного события равна единице P(Ω) =1.

Случайное событие называется **достоверным** если оно обязательно происходит при данном случайном эксперименте.

3. Вероятность невозможного события равна нулю P(∅) = 0.

Случайное событие считается **невозможным** если при данном эксперименте оно не может произойти.

# **2) Случайные события, действия над случайными событиями**

Теория вероятности изучает неслучайные закономерности массовых случайных явлений. Причем, рассматривает те явления, которые могут быть неоднократно повторены в одинаковых условиях.

Набор условий называется **случайным экспериментом.**

Результаты случайного эксперимента называют **случайным событием или событием** ( обозн.: А, В, С).

**Случайное событие** – это то что может произойти или не произойти в результате ряда экспериментов.

Теория вероятности изучает явления обладающие статистической устойчивостью (эксперимент может повторяться многократно).

Множество всевозможных итогов случайного эксперимента называется **вероятностным пространством** ( + Ω={ ω1 ,ω2 ,…ωn})

Случайные события – это всегда подмножество вероятносного пространства.

**Для случайных событий определены алгебраические действия:**

1. Суммой, или объединением, двух событий А и В называется такое событие С , которое состоит в осуществлении события А или события В , или событий А и В вместе.

С = А + В, или С = А ∪ В .

Сумма событий A + B состоит из всех элементарных событий, принадлежащих событиям А и B.

2. Произведением, или пересечением, двух событий А и В называется событие С, которое состоит в осуществлении события А и события В одновременно.

С = АВ , или С = А ∩ В .

Произведение событий AB состоит из элементарных событий, одновременно входящих в событие A и событие B .

3.  – **противоположное событие** – событие при котором событие А никогда не произойдет

# **3) Теорема сложения и умножения вероятностей. Совместные и несовместные события. Зависимые и независимые события**

События А и В называются **совместными**, если они могут появиться одновременно в одном и том же испытании. Это значит, что существуют такие элементарные события, которые входят в состав и А, и В одновременно, другими словами, произведение событий AB не пустое множество.

События А и В называются **несовместными**, если появление одного из них исключает появление другого, т. е. если АВ = ∅. Иными словами, нет ни одного элементарного события, которое входило бы в состав и А, и В одновременно. В частности, противоположные события A и A всегда несовместны.

Два события А и В называются **зависимыми**, если вероятность появления одного из них зависит от наступления или не наступления другого.

В противном случае события А и В называются **независимыми**. Несколько событий называются независимыми в совокупности, если каждое из них и любая комбинация остальных есть события независимые.

**Теорема сложения вероятностей совместных событий**

*Вероятность суммы 2-х несовместных событий = сумме вероятностей этих событий. Для совместных событий вероятность суммы = сумме вероятностей этих событий - вероятность их совместного происхождения*

Р(А+В)=Р(А)+Р(В)\_Р(АВ)

Р()=1-Р(А) — вероятность происхождения противоположных событий

**Теорема умножения вероятностей**

*Вероятность произведения 2-х событий =произведение вероятности 1-го события на условную вероятность 2-го при условии что 1-е произошло.*

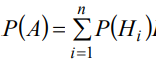
Р(АВ)=Р(А)\*Р(В|А)= Р(В)\*Р(А|В)

Вероятность произведения 2-х независимых событий = произведению вероятностей этих событий

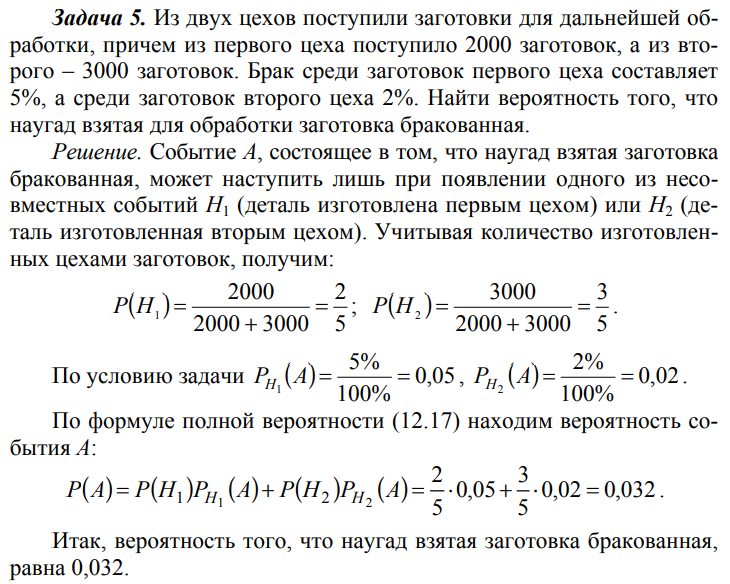
# **4) Формула полной вероятности. Примеры**

Пусть событие А происходит при условии происхождения 1-го из событий Н1, Н2,…,Нп. которые попарно несовместны и образуют полную группу.

Событие Нi называется **гипотезой** когда вероятность события А = сумме произведения вероятностей гипотез на условную вероятность события а при условии, что данная гипотеза произошла.



\*Р(А|Нi)

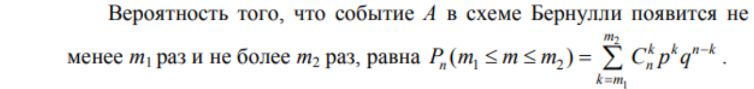


# **5) Схема Бернулли. Предельные теоремы в схеме Бернулли**

Пусть производится n независимых испытаний, в каждом из которых событие А может появиться с вероятностью р или не появиться с вероятностью q =1 – p. В этом случае говорят, что имеет место *схема испытаний Бернулли*.

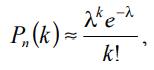
Вероятность того, что в описанных n испытаниях событие А появиться ровно k раз (0 ≤ k ≤ n) , вычисляется по формуле Бернули:



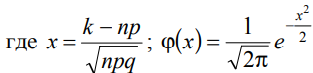


Если после независимых испытаний проводимых достаточно большое число раз, то в формуле Бернули появляются большие числа и требуется больший обьем вычислений в этом случае используются **предельные теоремы**:

- если число испытаний велико, а вероятность происхождения события мала, то используется формула Пуасона:

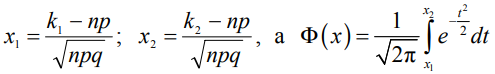
 

- если вероятность не является малой, то используется локальная теорема Муавра Лапласа:



- Если вероятность р появления события А в каждом испытании постоянна и не близка к нулю или единице, то вероятность Pn (k1 ; k2) того, что событие А появится в п испытаниях от k1 до k2 раз, вычисляется по формуле





# **6) Определение случайной величины. Функция распределения СВ и ее свойства**

Случайной величиной называют величину, которая в результате испытания принимает одно и только одно возможное значение, наперед неизвестное и зависящее от случайных причин, которые заранее не могут быть учтены.

Случайные величины обычно обозначают греческими буквами ξ, η, ζ,… или заглавными буквами X, Y, Z,… латинского алфавита, а их возможные значения – строчными латинскими буквами x, y, z,….

Случайные величины делятся на *дискретные* и *непрерывные*.

**Дискретной** называют случайную величину, если ее возможные значения можно пронумеровать. Дискретная случайная величина принимает изолированные значения.

**Непрерывной** называют случайную величину, которая может принимать все значения из некоторого конечного или бесконечного промежутка.

**Законом распределения** случайной величины называется любое соответствие между возможными значениями случайной величины и их вероятностями. Это соответствие можно задать таблицей, графически и аналитически

При табличном способе задания *дискретной случайной величины* в первой строке указывают ее возможные значения, а во второй – их вероятности



Законы распределения как дискретных, так и непрерывных случайных величин можно задать с помощью интегральной функции распределения F(x).

*Интегральной функцией распределения случайной величины* ξ называется функция F(x), определяющая вероятность того, что случайная величина ξ примет значение, меньшее х:



свойства F(x):

1) 

2) F(x) – неубывающая и непрерывная слева функция, т. е. если 

3) 

При решении задач наиболее часто используется следующее свойство F(x) :



# **7) Дискретные СВ, способы их задания**

**Дискретной** называют случайную величину, если ее возможные значения можно пронумеровать. Дискретная случайная величина принимает изолированные значения.

При табличном способе задания *дискретной случайной величины* в первой строке указывают ее возможные значения, а во второй – их вероятности



Следует иметь в виду, что . Такую таблицу называют также *рядом распределения дискретной случайной величины*.

Законы распределения как дискретных величин можно задать с помощью интегральной функции распределения F(x).



**Математическим ожиданием** дискретной случайной величины ξ называют сумму произведений всех ее возможных значений на их вероятности:



Для дискретной случайной величины **дисперсия** вычисляется по формуле



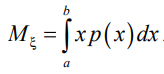
# **8) Непрерывные СВ, способы их задания**

**Непрерывной** называют случайную величину, которая может принимать все значения из некоторого конечного или бесконечного промежутка.

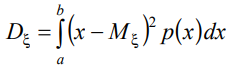
Законы распределения непрерывных величин можно задать с помощью интегральной функции распределения F(x).



**Математическим ожиданием** непрерывной случайной величины ξ, возможные значения которой принадлежат отрезку [a; b], называют определенный интеграл



Для непрерывной случайной величины **дисперсия** равна



если возможные значения принадлежат отрезку [a; b], и

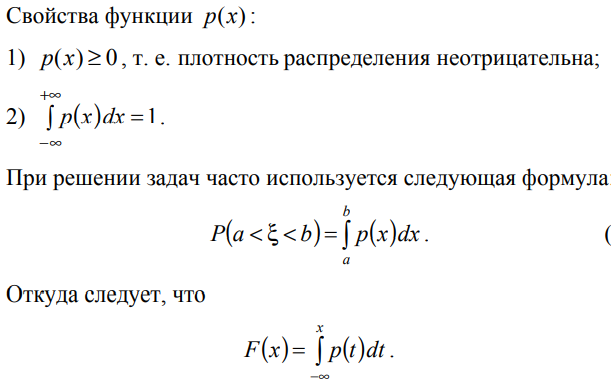


если возможные значения принадлежат всей оси Ох.

# **9) Плотность распределения СВ и ее свойства**

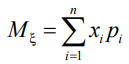
Плотностью распределения вероятностей, или дифференциальной функцией распределения, непрерывной случайной величины называется функция p(x), такая, что



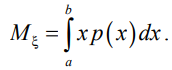


# **10) Математическое ожидание СВ, формулы для вычисления**

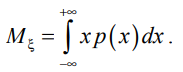
*Математическим ожиданием дискретной случайной* *величины* ξ называют сумму произведений всех ее возможных значений на их вероятности



Математическим ожиданием непрерывной случайной величины ξ, возможные значения которой принадлежат отрезку [a; b], называют определенный интеграл



Если возможные значения принадлежат всей оси Ох, то



Вероятностный смысл математического ожидания состоит в том, что оно приближенно равно среднему ожидаемому значению случайной величины.

Отклонением случайной величины от ее математического ожидания называют разность ξ − Mξ между случайной величиной и ее математическим ожидание

# **11) Дисперсия СВ и ее свойства. Среднеквадратическое отклонение**

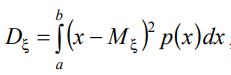
Дисперсией (рассеиванием) случайной величины называют математическое ожидание квадрата отклонения случайной величины от ее математического ожидания:



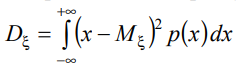
Для дискретной случайной величины дисперсия вычисляется по формуле



Для непрерывной случайной величины дисперсия равна



если возможные значения принадлежат отрезку [a; b], и



если возможные значения принадлежат всей оси Ох.

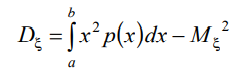
На практике, как правило, используют другие формулы. Поскольку верно, что



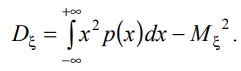
то дисперсия для дискретной случайной величины вычисляется по формуле



Для непрерывных случайных величин по формуле



или



Дисперсия характеризует степень рассеяния возможных значений случайной величины относительно ее математического ожидания.

# **12) Биномиальное распределение**

**Биноминальный закон распределения**

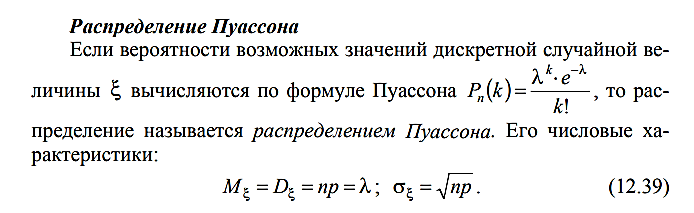
Если вероятности возможных значений дискретной случайной величины ξ вычисляются по формуле Бернулли , то распределение называется биноминальным. Числовые характеристики биноминального распределения:



# **13) РАСПРЕДЕЛЕНИЕ ПУАССОНА**

***Распределение Пуассона*** – это распределение числа появления редких случайных событий, которые могут принимать только два противоположных значения. Это распределение возникает, когда вероятность наступления одного из признаков мала, а число испытаний **n** большое. Если известна вероятность успеха **p** в каждом испытании, то вероятность того, что в **n** независимых испытаниях событие наступит **k** раз. Т.е. это распределение вероятностей случайной величины Х с целочисленными неотрицательными значениями k=0,1,2,.., заданное формулой

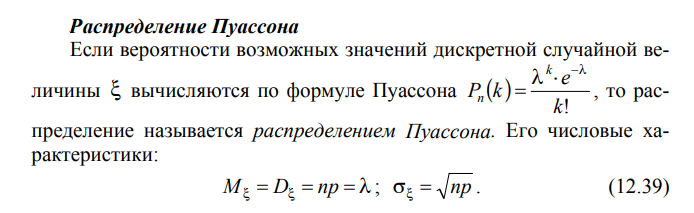
Его числовые характеристики:

 , где

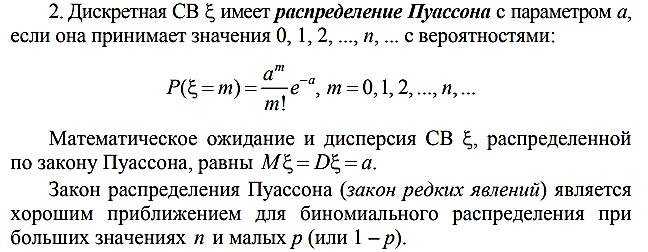
– параметр распределения

ξ – вероятность возможных значений дискретной случайной величины

– математическое ожидание

* стандартное отклонение

или может быть это-?



# **14) ГЕОМЕТРИЧЕСКОЕ РАСПРЕДЕЛЕНИЕ**

Дискретная случайная величина   имеет ***геометрическое распределение*** с параметром , если она принимает значения  0,1,2, ..., m, … (бесконечное, но счетное множество значений) с вероятностями:

Вероятности *Рm*для последовательности значений *m* образуют геометрическую прогрессию с первым членом *p* и знаменателем *q.*

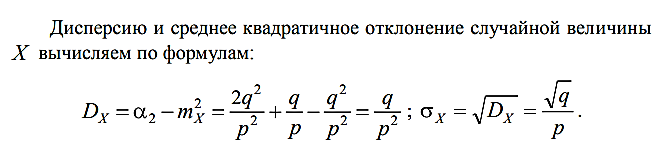
На практике геометрическое распределение появляется при независимых испытаниях с целью получения положительного результата – наступления события *А,* вероятность появления которого =*р.* СВ Х – число неудачных попыток – имеет геометрическое распределение. В этом случае имеем:

Р{X=0}=P{первая попытка успешная}=p;

*…*

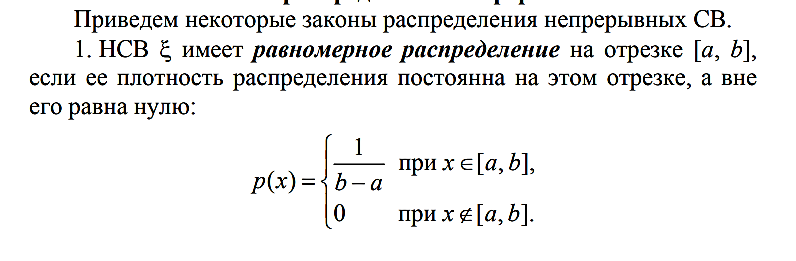
Ряд геометрического распределения случайной величины имеет вид:

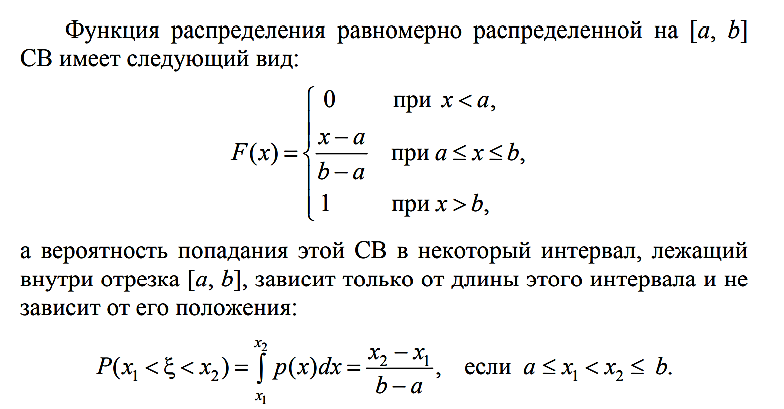
|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| xi | 1 | 2 | 3 | … | m | … |
| p­i | p | pq | pq2 | … | pqm-1 | … |

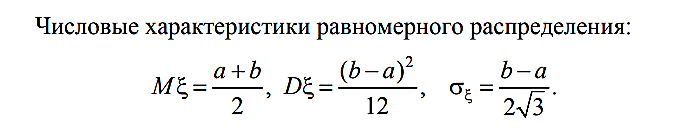


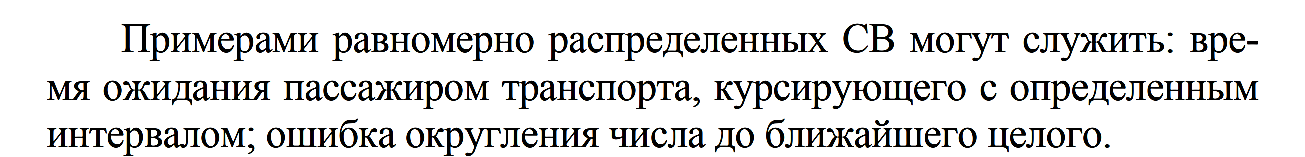
# **15) РАВНОМЕРНОЕ РАСПРЕДЕЛЕНИЕ**

***Равномерным распределением*** непрерывной случайной величины называется распределение, в котором значения случайной величины с двух сторон ограничены и в границах интервала имеют одинаковую вероятность. Это означает, что в данном интервале плотность вероятности постоянна. Т.е. СВ называется *равномерно распределенной* на [a,b], если её плотность вероятности на этом интервале постоянна, а вне [a,b] равна 0.



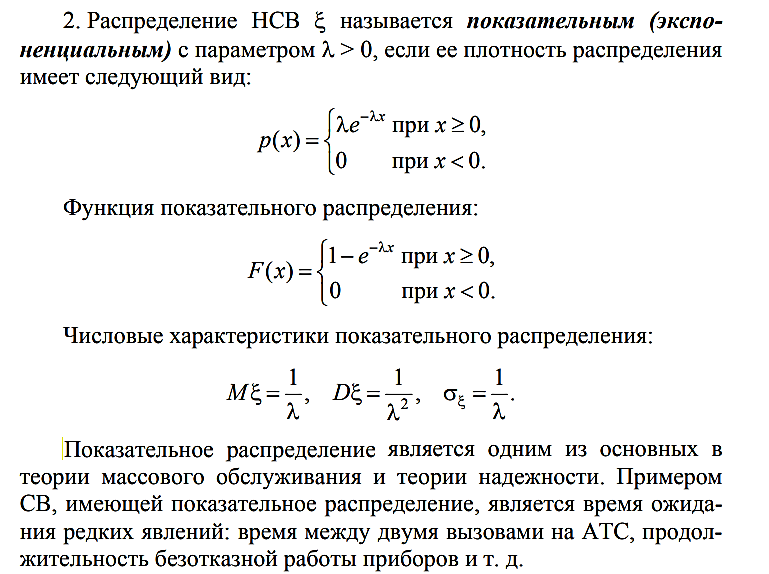


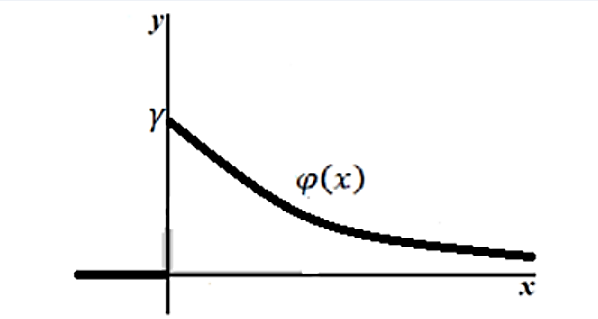


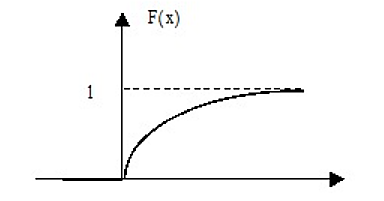
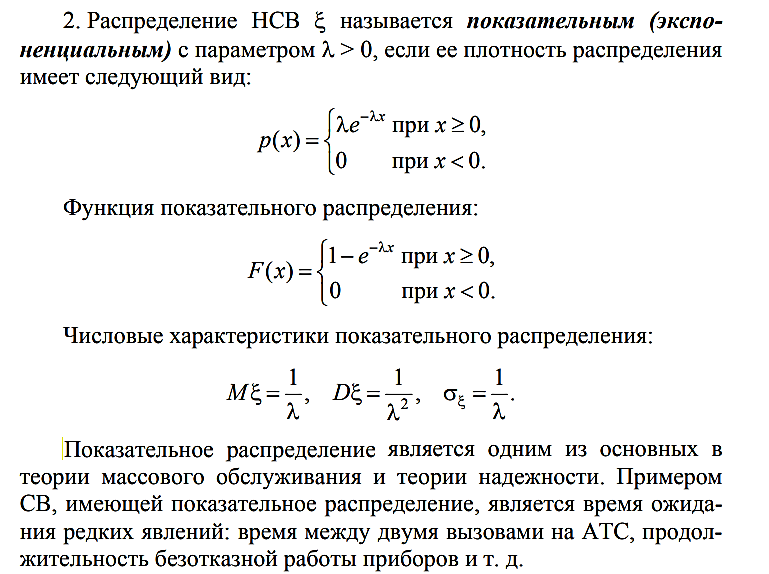


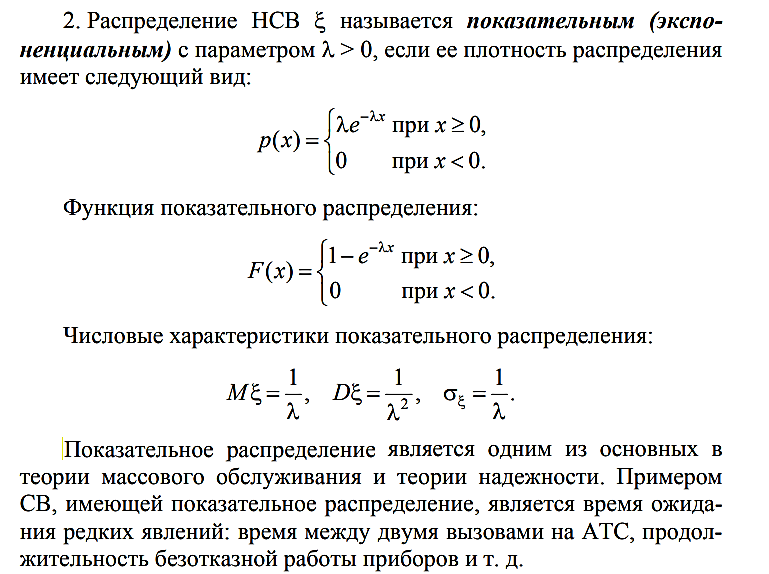
# **16) ПОКАЗАТЕЛЬНОЕ РАСПРЕДЕЛЕНИЕ**

***Показательным или экспоненциальным распределением***, называется распределение вероятностей непрерывной случайной величины х, которое описывается плотностью с параметром (единственным), в этом и есть его преимущество.



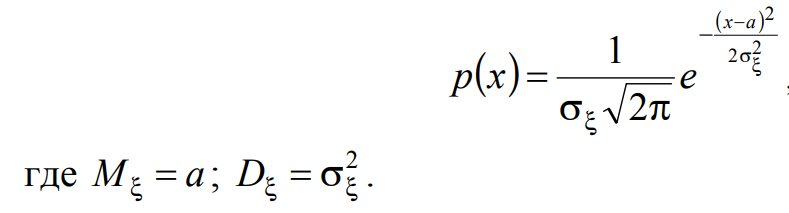
График плотности показательного распределения имеет вид

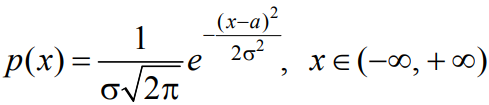
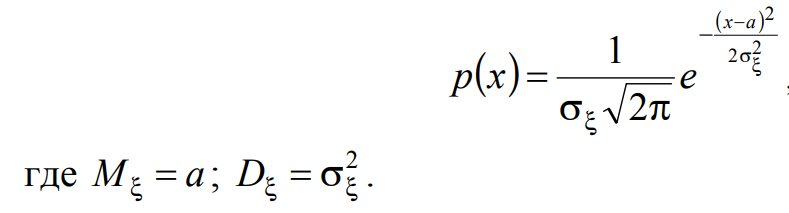


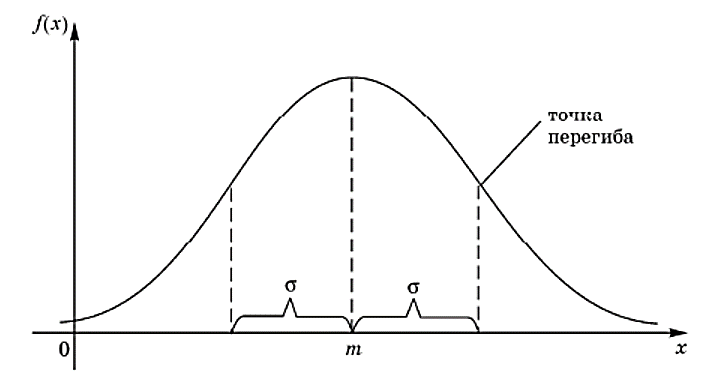


# **17) НОРМАЛЬНЫЙ ЗАКОН РАСПРЕДЕЛЕНИЯ. ПРАВИЛО ТРЕХ СИГМ**

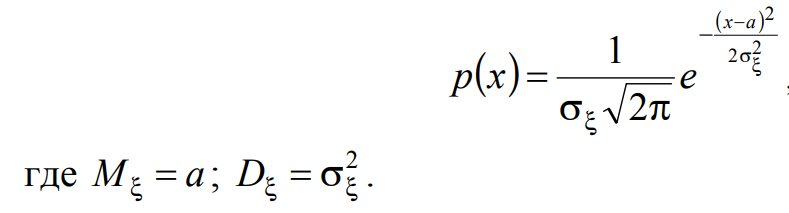
Нормальный закон распределения имеет плотность вероятности

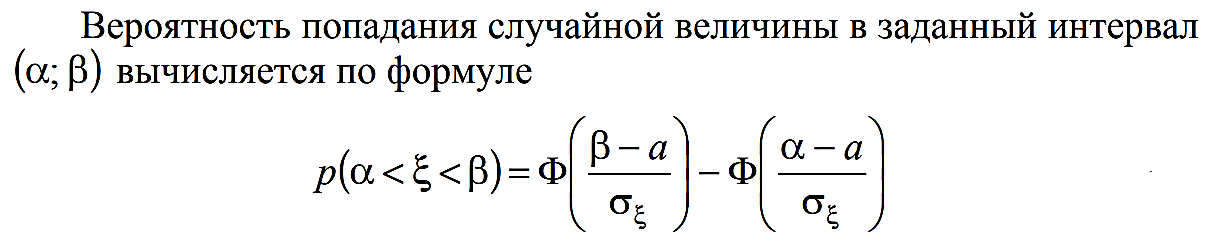


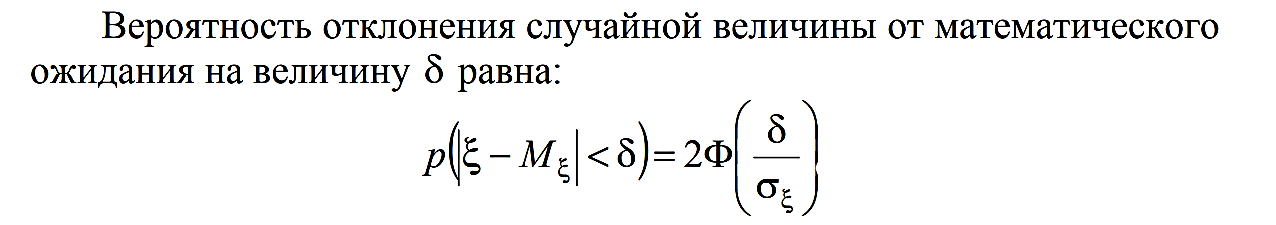


График функции плотности вероятности имеет максимум в точке x=m а точки перегиба отстоят от точки *m* на расстояние .

При    функция асимптотически приближается к нулю.

Помимо геометрического смысла, параметры нормального закона распределения имеют и вероятностный смысл. Параметр *m* равен математическому ожиданию нормально распределенной случайной величины, а дисперсия .

Вероятность попадания случайной величины в заданный интервал вычисляется по формуле:

Вероятность отклонения СВ от математического ожидания на величину равна:

Используя табличные значения ф-ии Лапласа, найдем вероятность

. Эту особенность нормального распределения называют “***правилом трех сигм***”:

***Правило трех сигм***: Если СВ имеет нормальный закон распределения с параметрами *а* и , то практически достоверно, что её значение заключены в интервале

Практическое применение правила :

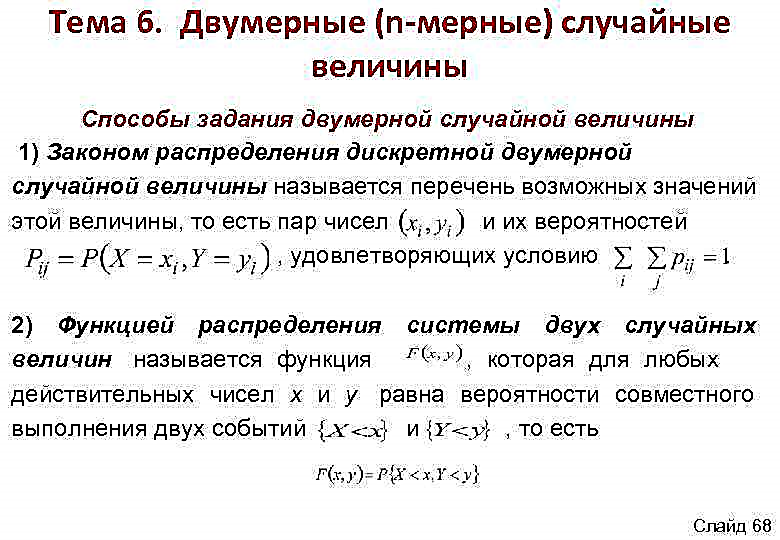
1. для оценки нормального распределения

2. для выявления ошибочно полученных результатов

3. для грубого определения

# **18) ПОНЯТИЕ О ДВУМЕРНОЙ СВ. ФУНКЦИЯ РАСПРЕДЕЛЕНИЯ ДВУМЕРНОЙ СВ И ЕЕ СВОЙСТВА**

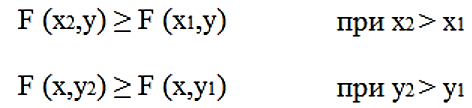
***Двумерной*** называют СВ (*X,Y*), возможные значения которой есть пары чисел (*x,у*). Составляющие *X* и *Y*, рассматриваемые одновременно, образуют систему двух случайных величин. При этом предполагаются определенными вероятности произведения событий *Х<x* и *Y<y* для любых вещественных *x,y.* Одномерные СВ *X,Y* называются компонентами двумерной СВ (*X,Y*).



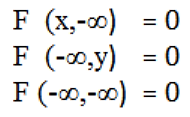
Свойства функции распределения двумерной случайной величины:

1.Функция 0 ≤ F(x,y) ≤ 1, т.е. величина неотрицательная меньше 1.

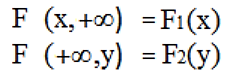
2.Функция F(x,y) есть возрастающая функция по каждому из аргументов.



3.Функция распределения F(x,y) = 0, если хотя бы один из аргументов x или y стремится к минус бесконечности.



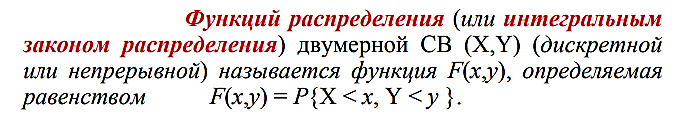
4.Функция F(x,y) равна функции от одного аргумента F(x) (F(y)), если y (x) стремится к бесконечности.

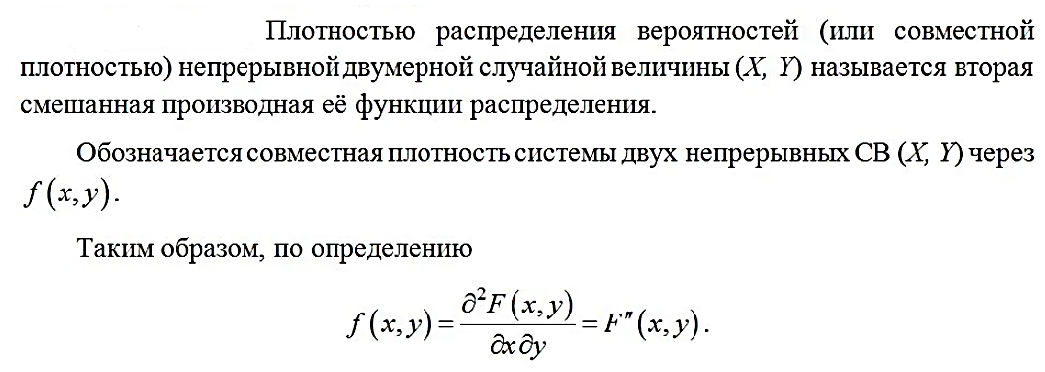


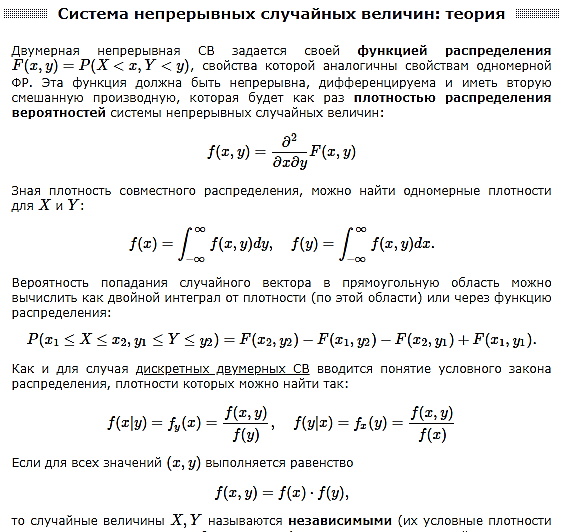
5. Функция F(x,y) равна 1, если оба аргумента стремятся к плюс бесконечности.

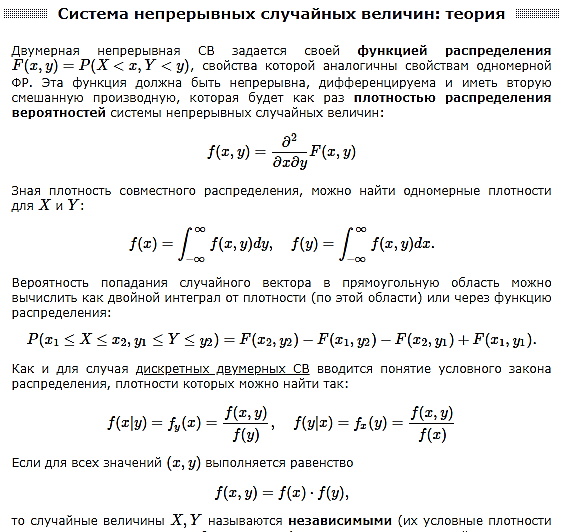


# **19) РАСПРЕДЕЛЕНИЕ НЕПРЕРЫВНОЙ ДВУМЕРНОЙ СВ. СОВМЕСТНАЯ ПЛОТНОСТЬ РАСПРЕДЕЛЕНИЯ. РАСПРЕДЕЛЕНИЕ СВ ПО ОТДЕЛЬНОСТИ**

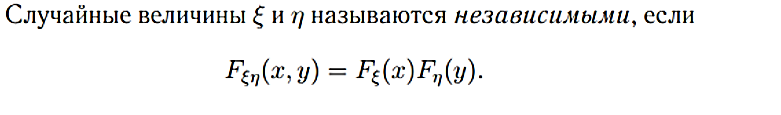
****

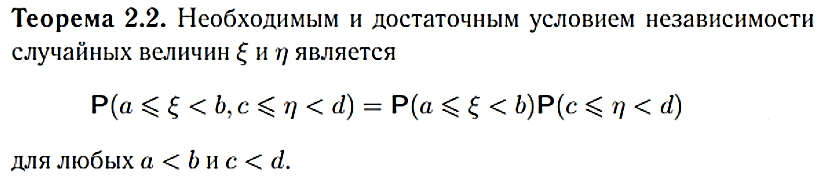


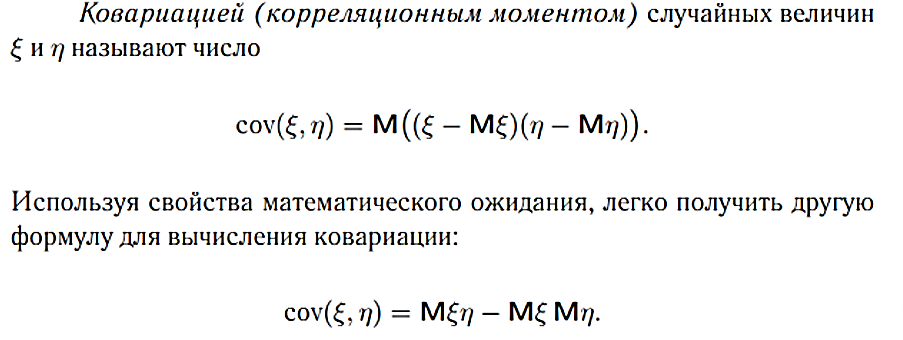
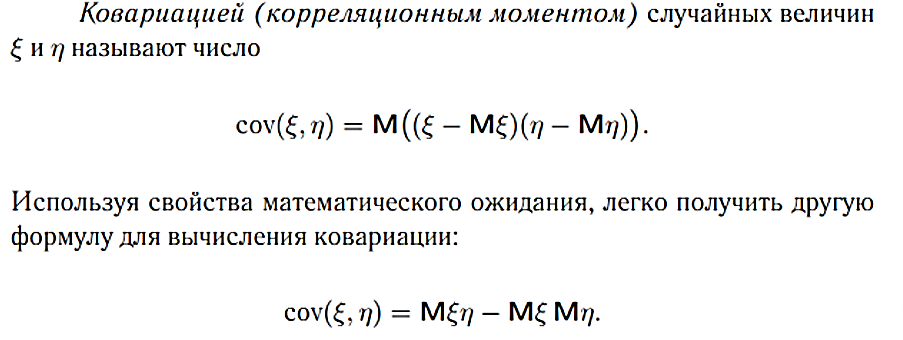
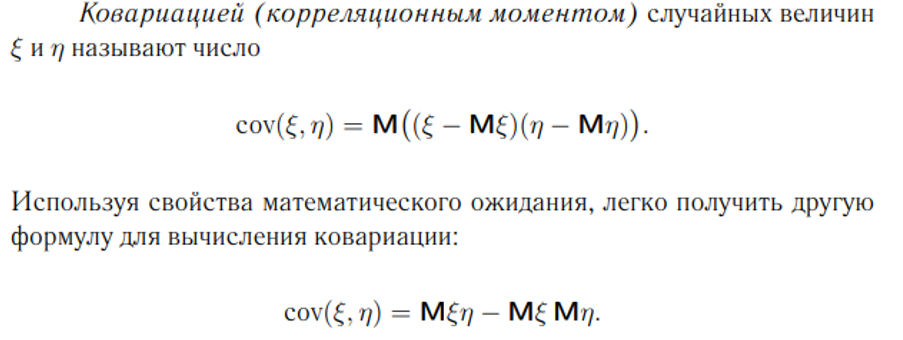




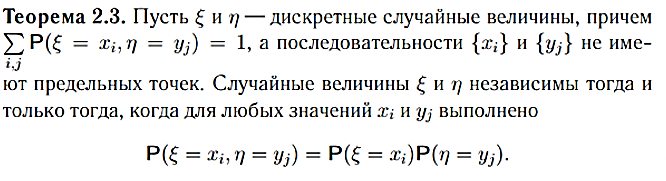
# **20) УСЛОВИЕ НЕЗАВИСИМОСТИ И НЕКОРРЕЛИРУЕМОСТИ СВ "ПСИ" И "ЭТА", СВЯЗЬ МЕЖДУ НИМИ**

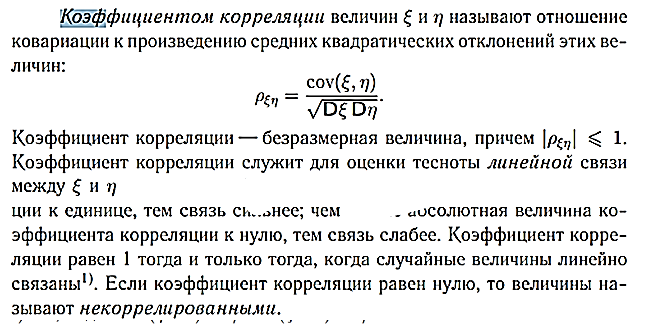




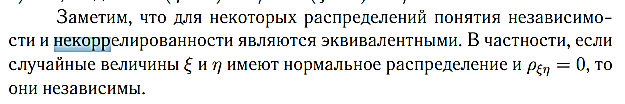
Ковариацией(корреляционным моментом) СВ называют число

Используя св-ва мат ожидания, получ ф-лу



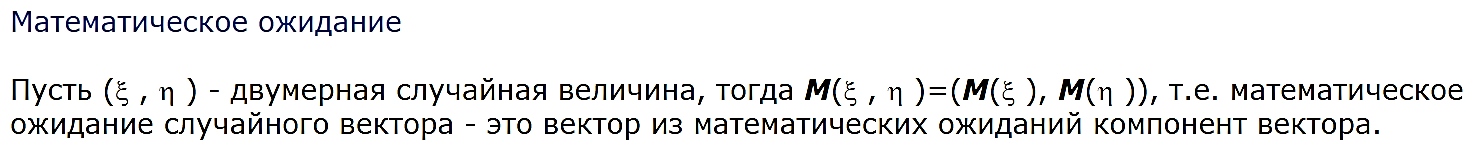


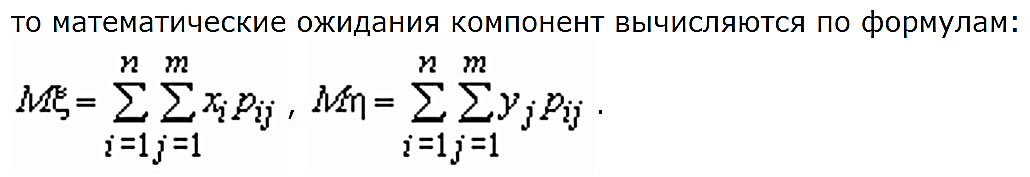
Если коэффициент корреляции =0, то величины называют *некоррелированными*.

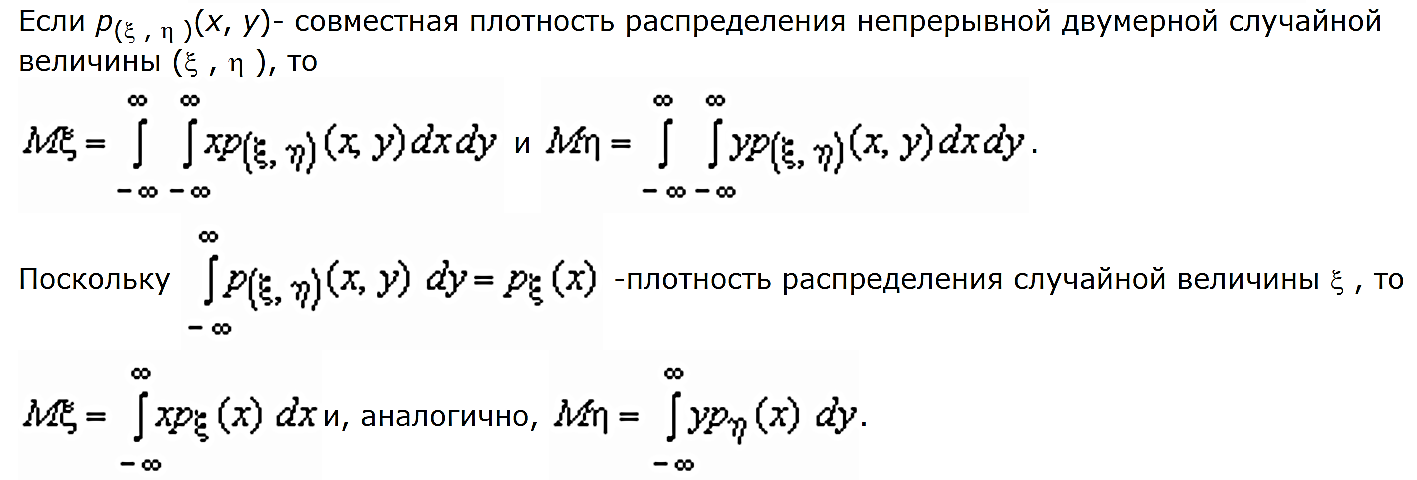


# **21) ЧИСЛОВЫЕ ХАРАКТЕРИСТИКИ ДВУМЕРНЫХ СВ "ПСИ" И "ЭТА", МАТЕМАТИЧЕСКОЕ ОЖИДАНИЕ, ДИСПЕРСИЯ, СИГМА, КОВАРИАЦИЯ СВ**

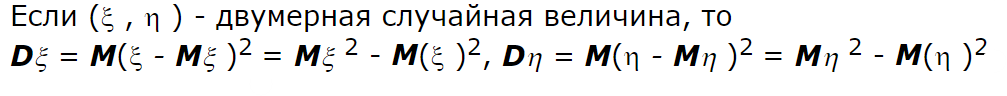
Среди числовых характеристик двумерной случайной величины важнейшими являются условное математическое ожидание и ковариация.





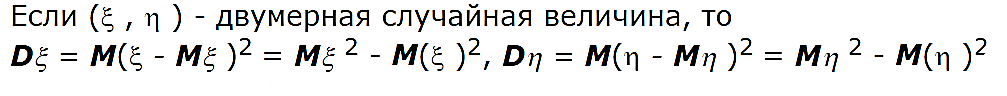


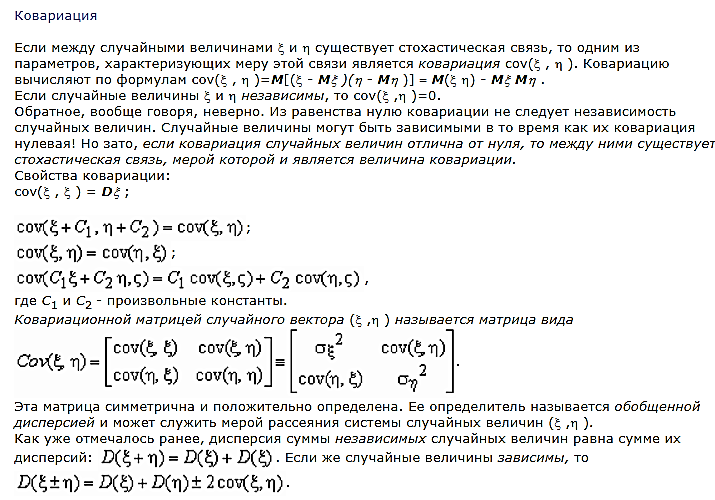
***Дисперсией*** (рассеянием) случайной величины называется математическое ожидание квадрата ее отклонения от ее математического ожидания.



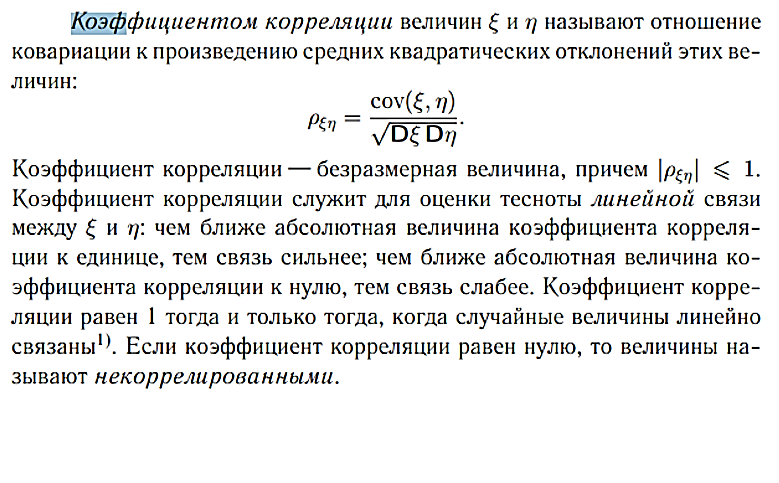
Если между случайными величинами "ПСИ" И "ЭТА" существует стохастическая связь, то одним из параметров, характеризующих меру этой связи является *ковариация.* ***Ковариацию*** вычисляют по формулам



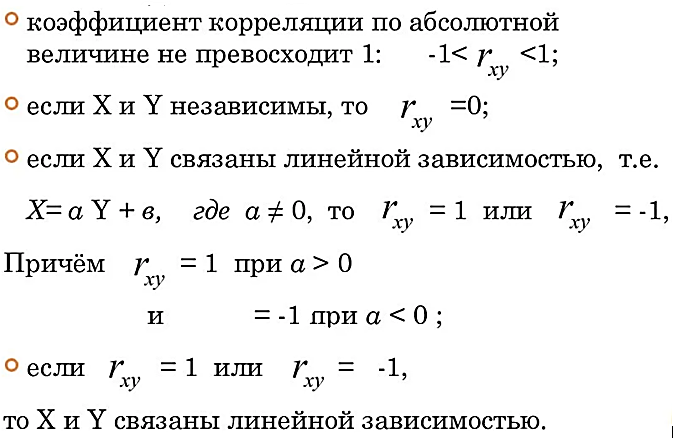
Если случайные величины *независимы*, то =0



# **22) КОЭФФИЦИЕНТ КОРРЕЛЯЦИИ СВ И ЕГО СВОЙСТВА**



***Свойства коэффициента корреляции СВ:***

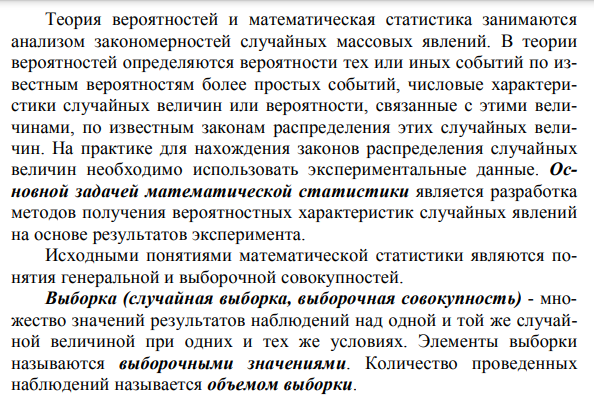


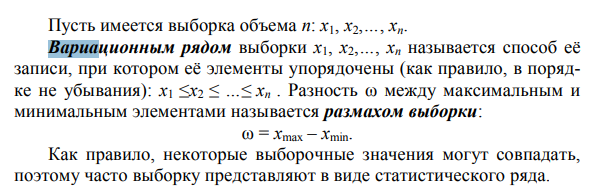
# **23) ОСНОВНЫЕ ЗАДАЧИ МАТЕМАТИЧЕСКОЙ СТАТИСТИКИ. ВЫБОРКА, ВАРИАЦИОННЫЙ РЯД**

Математическая статистика изучает закономерности, которые имеют место в массовых совокупностях однородных объектов.

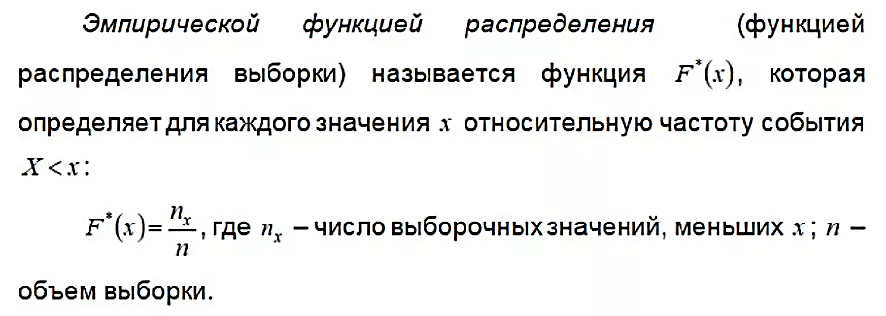
***Основные задачи математической статистики***: 1. Разработка методов сбора и группировки статистических сведений, полученных в результате наблюдений или в результате специально поставленных экспериментов. 2. Разработка методов анализа статистических данных в зависимости от целей исследования.

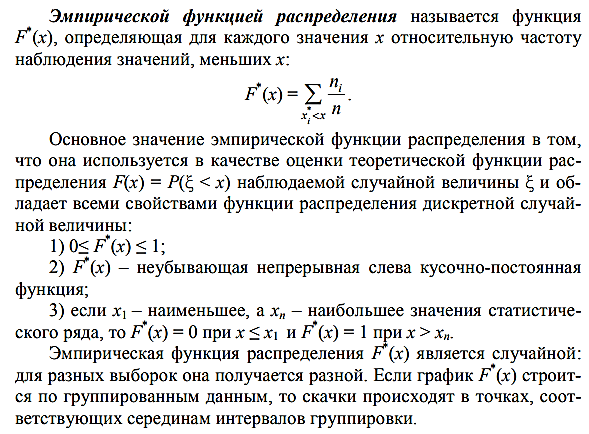
Т.е. разработка методов получения вероятностных характеристик случайных явлений на основе результатов эксперимента. Исходными понятиями математической статистики являются понятия генеральной и выборочной совокупностей.



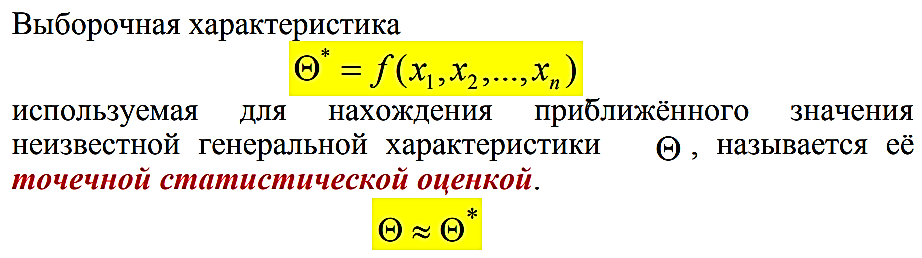


# **24) ЭМПИРИЧЕСКАЯ ФУНКЦИЯ РАСПРЕДЕЛЕНИЯ И ЕЕ СВОЙСТВА**





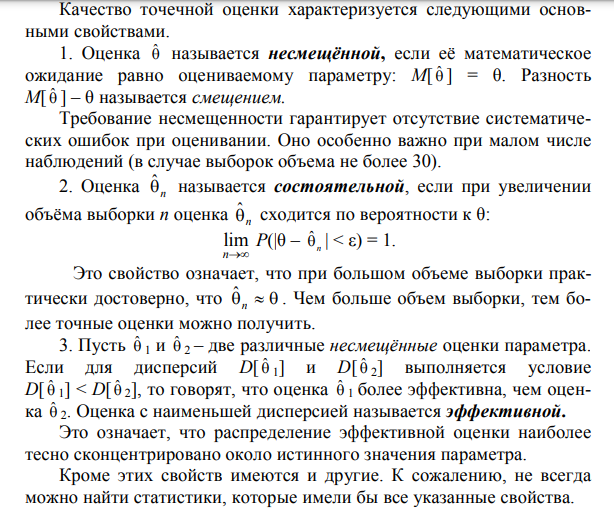
# **25) ТОЧЕЧНАЯ ОЦЕНКА ПАРАМЕТРОВ РАСПРЕДЕЛЕНИЯ, ИХ СВОЙСТВ**

 **Точечной** называют статистическую оценку, которая определяется одним числом. Точечная оценка характеризуется **свойствами:** несмещенность, состоятельность и эффективность.

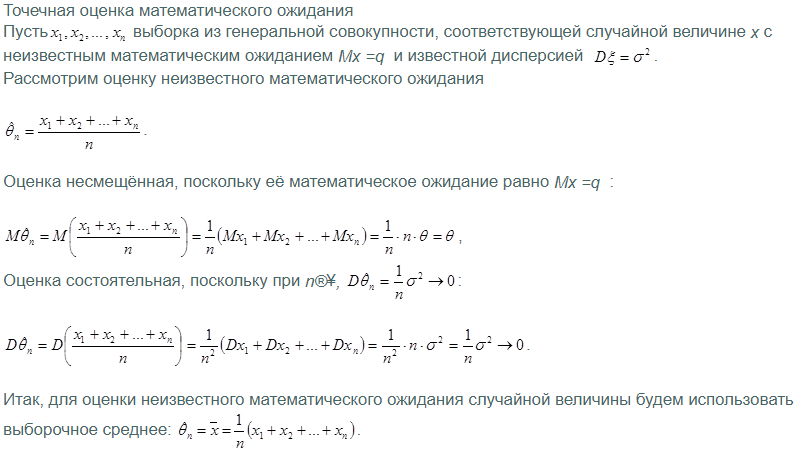
**Несмещенной** называют точечную оценку, математическое ожидание которой равно оцениваемому параметру при любом объеме выборки.

Точечная оценка называется ***состоятельной***, если при неограниченном увеличении объема выборки (*n* ® ¥) она сходится по вероятности к истинному значению параметра, то есть стремится к истинному значению оцениваемого параметра генеральной совокупности.

**Эффективной** называют точечную оценку, которая (при заданном объеме выборки *n*) имеет наименьшую возможную дисперсию, те есть гарантирует наименьшее отклонение выборочной оценки от такой же оценки генеральной совокупности.

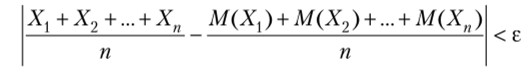


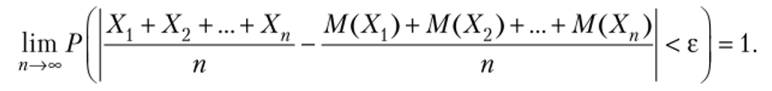
# **26) Точечная оценка математического ожидания, его свойства**



a - математическое ожидание нормального закона

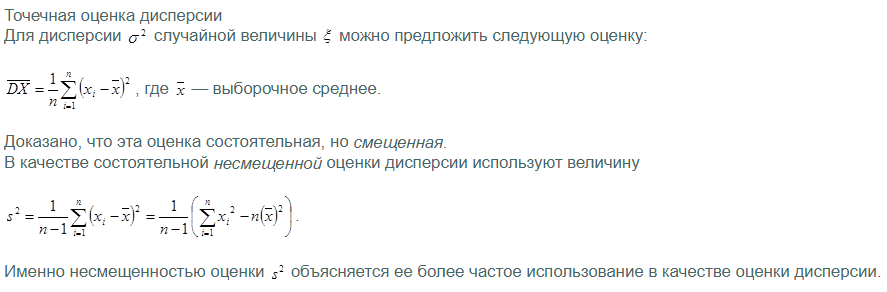
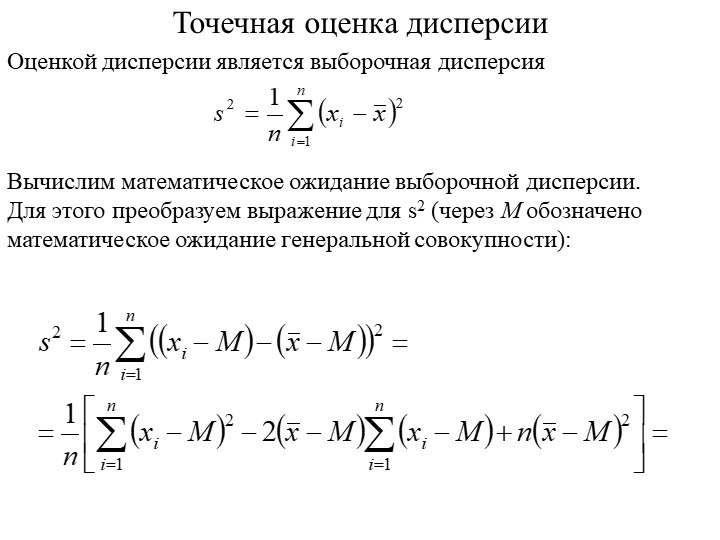
По теореме Чебышева является состоятельной оценкой математического ожидания. Теорема Чебышева. Если X1,X2,…Xn — попарно независимые случайные величины, причем дисперсии их равномерно ограничены (не превышают постоянного числа С), то, как бы мало ни было положительное число е, вероятность неравенства



будет как угодно близка к единице, если число случайных величин достаточно велико.

Если рассматривается достаточно большое число независимых случайных величин, имеющих ограниченные дисперсии, то почти достоверным можно считать событие, состоящее в том, что отклонение среднего арифметического случайных величин от среднего арифметического их математических ожиданий будет по абсолютной величине сколь угодно малым.

# **27) Точечная оценка дисперсии, формула ее вычисления, свойства**



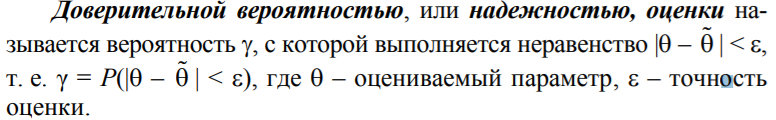
Отметим, что выборочная дисперсия является смещенной оценкой генеральной дисперсии. М(=

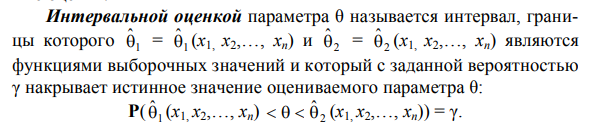
Поэтому рассмотрим исправленную выборочную дисперсию

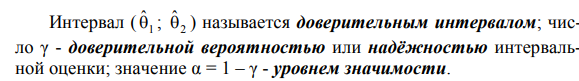
Dисправл выб = Эта дисперсия является состоятельной и эффективной оценкой генеральной дисперсии.

# **28) Интервальные оценки доверительной вероятности**

Интервальной называют оценку, которая определяется двумя числами – началом и концом интервала. Интервальные оценки позволяют установить точность и надежность оценок.

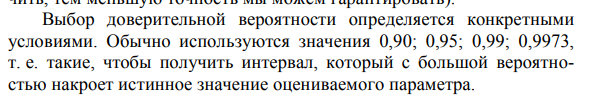






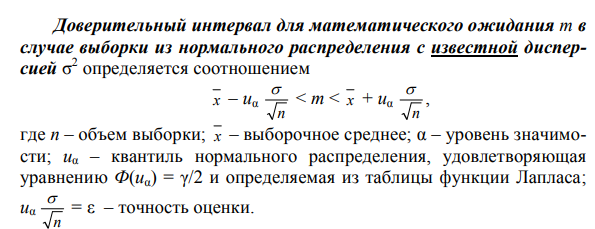
Доверительную вероятность обычно берут близко к 1. Т.к концы доверительного интервала случайны, мы можем доверительным интервалом называть такой интервал, который с заданной вероятностью покрывает значение оцениваемого параметра. Обычно его берут симметричным. Для построения доверительного интервала необходимо знать/предполагать закон распределения генеральной совокупности (для точечных он не требовался). Доверительный интервал для наизвестного мат.ожидания нормального распредеения случайной величины при известной дисперсии

n – объем выборки, = =, -квантираспределение Лапласа при значении





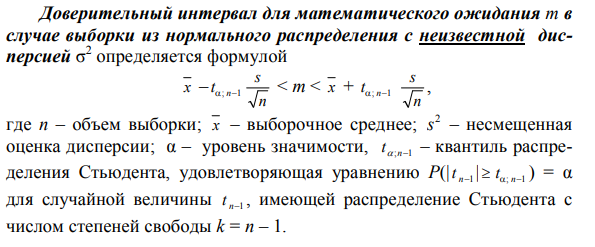
# **29) Доверительный интервал для неизвестного математического ожидания нормального распределения СВ при известной дисперсии**



Доверительный интервал — это интервал, построенный с помощью случайной [выборки](http://www.machinelearning.ru/wiki/index.php?title=%D0%92%D1%8B%D0%B1%D0%BE%D1%80%D0%BA%D0%B0) из распределения с неизвестным параметром, такой, что он содержит данный параметр с заданной вероятностью.

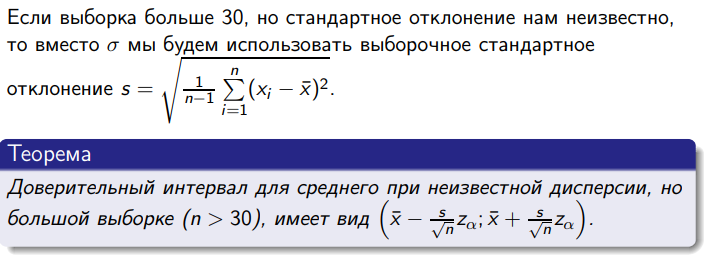
# **30) Доверительный интервал для неизвестного математического ожидания нормального распределения СВ при НЕизвестной дисперсии**

Доверительный интервал — это интервал, построенный с помощью случайной [выборки](http://www.machinelearning.ru/wiki/index.php?title=%D0%92%D1%8B%D0%B1%D0%BE%D1%80%D0%BA%D0%B0) из распределения с неизвестным параметром, такой, что он содержит данный параметр с заданной вероятностью.





Обычно уровень значимости равен 0.01, 0.05, 0.1.

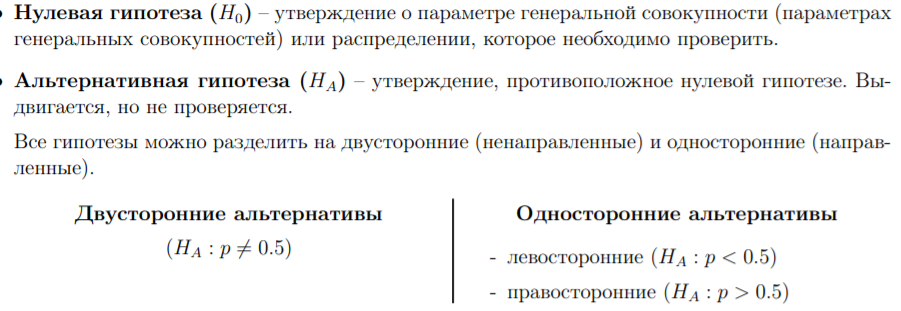




# **31) Проверка статистических гипотез**

Цель статистической проверки гипотез состоит в том, чтобы на основании выборочных данных принять решение о справедливости основной гипотезы Н0. Гипотезы называются статистическими, если они касаются параметров СВ или вида ф-ии распределения, к-е формулируются на основании выборки. Если з.распределения выборки известен и рассм. Гипотеза о параметрах этого закона, то такая гипотеза называется параметрической. Если рассм. Вопрос о неизвестном з.распределения генеральн.совокупности, то говорят о непараметрических гипотезах.Статистическая гипотеза – простая,если она содержит только 1 предположение.





**Проверка гипотезы о равенстве мат ожидания заданному значению (**критерий Стьюдента**)**. **Проверка гипотезы о равенстве (может ещё быть а) больше, б) меньше) заданному значению дисперсии норм. Распределения (**Критерий хи-квадрат**).**  
**Сравнение двух дисперсий нормально распределённых случайных величин**(критерий Фишера). **Сравнение нескольких дисперсий нормально распределённых случайных величин, если объём выборок одинаковый (**критерий Кофмана**). Сравнение двух математических ожиданий в случаи независимых нормально распределённых случайных величин.** Этот критерий используется, когда мы хотим, например, узнать, дают ли два способа, две технологии и т.д. одинаковый результат. Тогда используем этот критерий. И, выбрав этот критерий, нужно сначала проверить однородность дисперсий, т.е. проверить 3 критерий выборок. Если приняли гипотезу 3-его критерия, то использовать 5-ый критерий.

Для проверки статистических гипотез по данным выборки находят частное значение критерия Кнаблюдаемое, после выбора определенного статистич.критерия множество его возможных значений разбивают на 2 непересекающ. множества, одно из к–х назыв обл принятия гипотезы или обл допустимого значения критерия, второе – критическая область. Это такая совокупность значений критерия К, при котором нулевую гипотезу отвергают.

Соотв. областью принятия гипотезы называют совокупность значений критерия К, при котором нулевую гипотезу принимают.

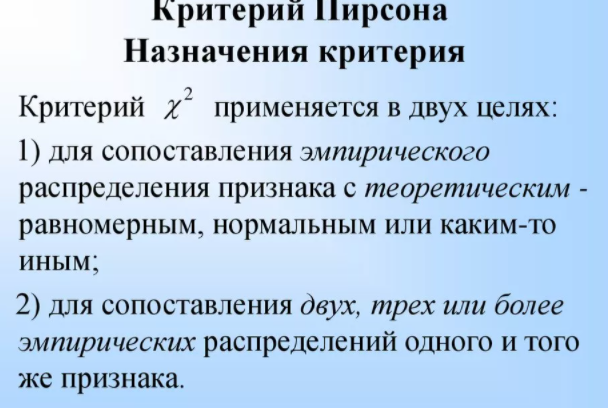
Если наблюдаемое значение статистического критерия Кнабл. критической области, то нулевую гипотезу Н0 отвергают в пользу альтернативной. Иначе нет оснований по выборке отвергнуть гипотезу.

# **32) Критерий Пирсона**

Критерий Пирсона - это универсальный метод математической статистики. Он применяется для оценки значимости различий между двумя или несколькими относительными признаками. **Это критерий согласия.**

. Сравнивается с табличной величиной , *l* – число параметров распределения, определяемых по выборке.

Если предполагаемое распределение имеет нормальный закон распределения, то число степеней свободы оценивают по двум параметрам (математическое ожидание и среднеквадратическое отклонение) и формула имеет вид: **k=*l*−3**



Алгоритм:

1. Выбор теоретического закона распределения (обычно задан заранее, если не задан - анализируем выборку, например, с помощью гистограммы относительных частот, которая имитирует плотность распределения).

2. Оцениваем параметры распределения по выборке (для этого вычисляется математическое ожидание и дисперсия): a, σ для нормального, a, b - для равномерного, λ - для распределения Пуассона и т.д.

3. Вычисляются теоретические значения частот (через теоретические вероятности попадания в интервал) и сравниваются с исходными (выборочными).

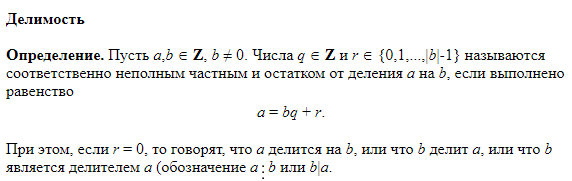
4. Анализируется значение статистики χ2 и делается вывод о соответствии (или нет) теоретическому закону распределения.

**Если хи-квадрат наблюдаемое будет меньше хи-квадрат табличное, то мы принимаем гипотезу.**

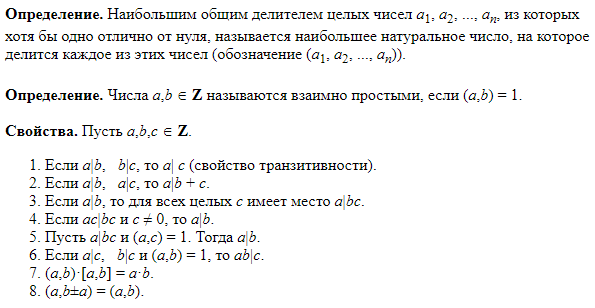
Критерий Пирсона, или критерий χ2(Хи-квадрат) - применяют для проверки гипотезы о соответствии эмпирического распределения предполагаемому теоретическому распределению F(x) при большом объеме выборки (n ≥ 100). Критерий применим для любых видов функции F(x), даже при неизвестных значениях их параметров, что обычно имеет место при анализе результатов механических испытаний. В этом заключается его универсальность.

# **33) Целые числа. Свойства делимости. Простые числа и их свойства**

N={0,1,2,…} множество натуральных чисел, Z = {0, ±1,±2,…} множество целых чисел, Q={m/n, m, N\* = {1,2,..} – множество натуральных положительных чисел, R – множество действительных (вещественных чисел). **Целые числа** — это расширенное множество натуральных чисел, которое можно получить, если добавить к ним нуль и противоположные натуральным отрицательные числа. Множество целых чисел обозначают **Z**.



Для каждого a и b существуют числа q и r, такие что a=bq+r, r – остаток, q – частное. Если r=0, то говорят, что a делится на b, и a делится на q. Или говорят, что число a кратно числу b, b и q – называются делителями числа a.



Все целые числа делятся на 1. Все натуральные числа являются делителями нуля. Единственный делитель единицы – сама единица. Пусть целое число a делится на натуральное число m, а число m в свою очередь делится на натуральное число k, тогда a делится на k (свойство транзитивности деления). Натуральное число n>1 называется **простым**, если оно имеет в точности два различных натуральных делителя – 1 и n, в противном случае n называется составным. 1) Если простое число p делится на простое число q, то эти числа равны (p=q). 2) Если p- простое число, то любое натуральное число либо делится на p, либо взаимно простое с p. 3) Произведение натуральных чисел a и b делится на простое число p в том случае, когда хотя бы одно из этих чисел делится на p. 4) Любое натуральное число, отличное от 1, является либо простым, либо произведением простых чисел  
5) Среди простых чисел нет наибольшего, множество простых чисел бесконечно  
6) Если m\*n делится на простое число p , то m делится на p или n делится на p.

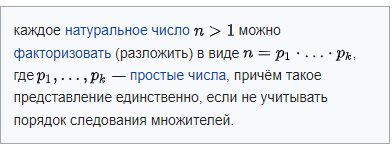
# **34) Критерий взаимной простоты чисел. Основная теорема арифметики**

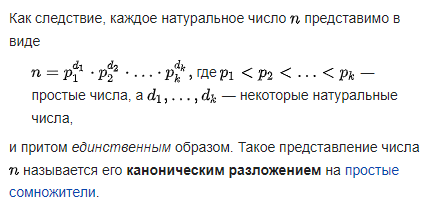
Простые числа делятся на себя и на единицу. Если число n>1 не делится ни на одно простое число p≤, то n – простое.

Два целых числа a и b называются взаимно простыми, если их наибольший общий делитель равен единице, то есть, НОД(a, b)=1. Проще говоря, взаимно простые числа — это целые числа, у которых нет общих делителей, кроме единицы. **Наибольшим общим делителем** двух чисел a и b называется наибольшее число, на которое a и b делятся без остатка. Для записи может использоваться аббревиатура НОД. Для двух чисел можно записать так: НОД (a, b). Числа, которые содержат больше двух множителей, то есть делятся на несколько чисел, называют **сложными**. Сложные числа состоят из перемноженных простых.

Любое целое положительное и отличное от единицы число a либо делится на простое число p, либо a и p – [взаимно простые числа](http://www.cleverstudents.ru/divisibility/coprime_numbers.html). Если произведение нескольких целых положительных и отличных от единицы множителей делится на простое число p, то хотя бы один множитель делится на p.

**Основная теорема арифметики** утверждает возможность разложения любого [целого числа](http://www.cleverstudents.ru/numbers/integers.html), которое больше единицы, на простые множители. Любое целое число, которое больше 1, можно разложить на произведение простых множителей, причем это разложение единственно, если не учитывать порядок следования множителей. Все составные числа, которые могут быть разложены на множители, представлены произведением простых чисел; то есть все их множители — простые числа.





# **35) НОК и НОД, алгоритм Евклида**

Наибольшим общим делителем чисел *a* и *b* называется наибольшее число, на которое *a* и *b* делятся без остатка. Обозначается (a,b). Наименьшее общее кратное (НОК) чисел *a* и *b —* это наименьшее число, которое кратно *a* и *b*. Другими словами, это такое маленькое число, которое делится без остатка на число *a* и число *b*.

Для любых чисел A и B, B≠0 существуют такие q, r, что A=B\*q+r, причем 0≤r<|B|. q называется полным частным, а r называется остатком от деления, они единственны. Алгоритм Евклида – это алгоритм нахождения наибольшего общего делителя (НОД) пары целых чисел.

Алгоритм Евклида заключается в построении ряда чисел следующего вида (|a|>|b|):   
a = b\*q1 + r1;

b = r1\*q2 + r2;

r1 = r2\*q3 + r3;

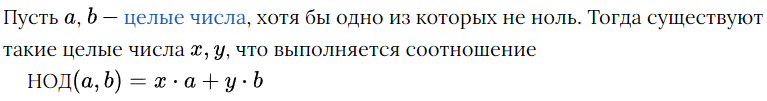
…

rn-1 = rn\*qn+1 + 0

Для нахождения наибольшего общего делителя двух чисел a и b (a и b – [целые положительные числа](http://www.cleverstudents.ru/numbers/integers.html#positive_and_negative), причем a больше или равно b) последовательно выполняется [деление с остатком](http://www.cleverstudents.ru/numbers/division_of_integers_with_remainder.html), которое дает ряд равенств вида  
  
Деление заканчивается, когда rk+1=0, при этом rk=НОД(a, b).

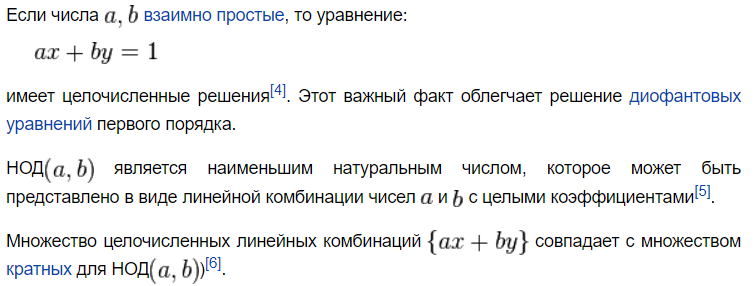
# **36) Соотношение Безу**

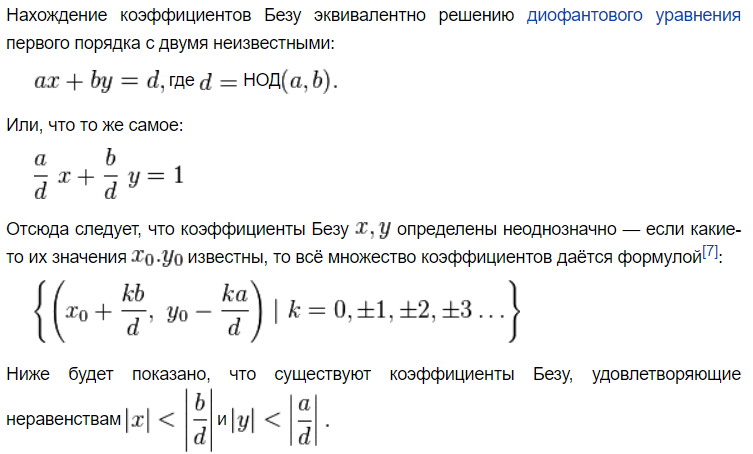
Соотношение Безу — соотношение между парой целых чисел и их [наибольшим общим делителем](https://dic.academic.ru/dic.nsf/ruwiki/8719). Это следует из алгоритма Евклида. НОД (a,b) = xa + yb, x, y – коэффициенты Безу. Числа a и b называются взаимно простыми, если их НОД = 1. Из соотношения Безу следует, что для взаимно простых чисел существуют числа au + bV = 1. Для взаимно простых чисел можем записать следующее свойство: 1) Если НОД (a1, a2, …, ak) = d, то (…, – взаимно простые числа. 2) Если число c делит произведение ab, и число c взаимно просто a, то c делит b, записывается c | a\*b и (c,a)=1, то c | b. 3) Если a и b1 взаимно простые, a и b2 тоже взаимно простые, то a взаимно просто b1\*b2, записывается (a,b1)=1, (a,b2)=1, то (a,b1\*b2)=1.





Следствие:





# **37) Диафантовые линейные уравнения**

Таким уравнением называется уравнение вида , где a1,a2,an,b – целые числа и решение ищут в целых числах. Чаще всего уравнение рассматривается относительно двух переменных ax+by=c. Если НОД (a,b) не существует, то уравнение не имеет решений. ax+by=c при условии (a,b)|c (НОД чисел a и b делим с c). . Шаги решения 1) Находим НОД (a,b) = d. 2) Проверяем, что c/d, если это так то 3) находим коэффициенты соотношения Безу au+bV=d 4) Умножаем обе части соотношения Безу на отношение , получаем , причем x0 =

Общее решение диафантового уравнения имеет вид:

# **38) Сравнение целых чисел. Свойства сравнений**

Пусть имеется произвольное число m. Тогда для любых чисел a и b равносильно следующее утверждение: 1) a и b имеют одинаковые остатки от деления на m

2) a-b делится на m, a-b=mq для некоторого целого q 3) a = b+mq Определение. Целые числа a и b называются сравнимыми по модулю m, если они удовлетворяют любому из трех условий, названных выше. Записывается a≡b(mod m). Сравнение обладает следующими свойствами: 1) Обеим частям сравнения можно прибавить/вычесть одно и то же число, a 2) Можно почленно складывать и вычитать сравнения по модулю, a≡b(mod m), c≡d(mod m) значит a =)mod m 3) Сравнение по модулю m можно почленно перемножать a≡b(mod m), c≡d(mod m) значит a\*c = (b\*d) mod m 4) Сравнение можно возводить в любую натуральную степень ak=bk(mod m) 5) Если сравнении a≡b(mod m) числа a,b,m имеют общий делитель d, то их можно на него сократить 6) Сравнение можно сократить на общий множитель a и b, если он взаимно простой с модулем m a=a1d, b=b1d, (d,m)=1. Тогда a≡b(mod m) => a1≡b1(mod m).

Также существуют такие свойства как 1) Рефлексивность сравнения a≡a(mod m) 2) Симметричность сравнения. Если a≡b(mod m), то b≡a(mod m) 3) Транзитивность (свойство переходит) Если a≡c(mod m), а c≡b(mod m), то a≡b(mod m). Эти 3 свойства означают, что отношение сравнимости на множестве целых чисел есть отношение эквивалентности. Это означает, что множество целых чисел разбивается на непересекающиеся классы попарно сравнимых друг с другом по mod m целых чисел. Каждый класс сравнимых друг с другом целых чисел характеризуется общими свойствами представителей этого класса: (a,m)=(b,m), если a≡b(mod m). Такие классы называются классами вычетов.

# **39) Множество классов вычетов**

Множество целых чисел разбивается на непересекающиеся классы попарно сравнимых др с др по mod m целых чисел. Каждый класс сравнимых друг с другом чисел характеризуется общими св-ми представителей этого класса.

(a,m)≡(b,m); если a≡b(mod m). Такие классы называют классами вычетов. При делении любого целого числа на число m cуществуют m-остатки: 0, 1, 2…m-1. Обозначать классы будем . Любой представитель конкретного класса полностью определяет свойства класса, множество всех классов называется множеством классов вычетов по mod m, обозначение Z/mZ={} Пусть , Z/mZ. Возьмем представителей k1, k2 ; *l*1, *l*2 . Тогда k1+k2 , *l*1+*l2*. А вот k1+ *l*1; k2+ *l*2. Аналогично с произведением. Сложение и умножение классов вычетов определяется через сложение и вычитание чисел, поэтому для них стандартные свойства: коммутативность, ассоциативность, существует нейтральный элемент по сложению и нейтральный элемент по умножению. Например Z/6Z ={}. Тогда + = , мы складываем 3+5 = 8 и делим на 6, остаток будет 2. В каждом множестве класса вычетов числа, которые дают одни остатки при делении на 1, 2 и так далее.

Для каждого класса существует противоположный класс по сложению. Если класс Z/mZ, (k,m) ≡1. Для каждого класса , отличного от 0, произведение \*≠0. Произведение k на любой из классов ≠ произведению k на другой класс. Существует обратимый класс k-1. Множество обратимых классов образует ПСВ (приведенную с-му вычетов). Z\*/mZ включает только те классы, остатки которых взаимно просты с m. Их количество – функция штук – описывается функцией Эйлера. Класс обратим, если найдется другой класс из класса вычетов, что обратим если существует Z/mZ, что \*=1 (в остатке дает 1 их произведение). обратимый к , он единственный, обратный класс определяется однозначно.

Класс Z/mZ обратим тогда и только тогда, когда представитель класса взаимно прост с m. Если m – простое число, то во множестве Z/mZ каждый ненулевой элемент обратим. Поскольку Z/mZ состоит из конечного числа элементов, то + и \* в нем можно задавать таблицами Кэли. Например, таблица Кэли для Z/6Z.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| + |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

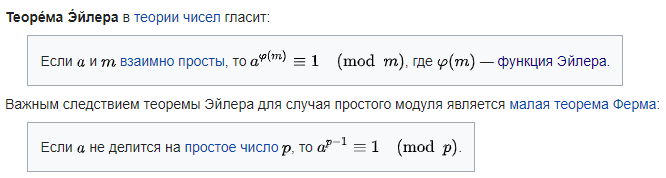
|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| \* |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

# **40) Функция Эйлера. Теорема Эйлера. Малая теорема Ферма**

Например, для числа 36 существует 12 меньших его и взаимно простых с ним чисел (1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35), поэтому  (36)=12. Функция Эйлера определена на множестве [натуральных чисел](https://ru.wikipedia.org/wiki/%D0%9D%D0%B0%D1%82%D1%83%D1%80%D0%B0%D0%BB%D1%8C%D0%BD%D0%BE%D0%B5_%D1%87%D0%B8%D1%81%D0%BB%D0%BE), и значения её лежат в множестве натуральных чисел. Чтобы вычислить , нужно перебрать все числа от 1 до p-1, и для каждого проверить, имеет ли оно общие делители с p, а затем подсчитать, сколько чисел оказались взаимно простыми с p. Свойства функции:

1) 2) 3) Если (n,m)=1 (m\*n) = (m) \* (n)

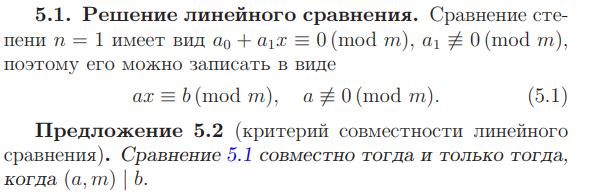
4) , n = – нахождение функции Эйлера.

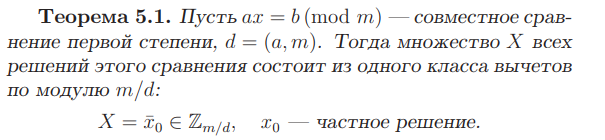


Функция Эйлера ставит в соответствие каждому натуральному числу m>1 количество натуральных чисел (<m), взаимно простых с m. Если, например, m=45, то функция Эйлера покажет, сколько чисел <45 взаимно просты с числом 45.

Малая теорема Ферма. Если p простое, a целое, НОД(a,p)=1 тогда и только тогда, когда (a,p)=1 ⬄ ap-1 -1 ≡ 0 (mod p).

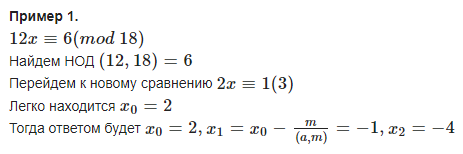
# **41) Решение линейных сравнений**





Решить сравнение — значит найти все удовлетворяющие ему х. Если х - решение сравнения, то решением является весь класс вычетов, содержащий х. Сравнения с одинаковым множеством решений называются равносильными. Пусть НОД(a,m)=d. Сравнение ax≡b(mod m) невозможно, если b не делится на d. При b, кратном d, сравнение имеет d решений.

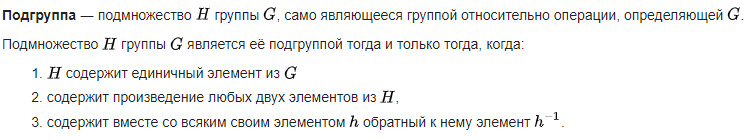
ax≡b(mod m), (a,b)=d. Составим новое сравнение x≡ (mod ), обозначим его adx≡bd(mod md) Пусть его решением будет x0, тогда остальные решения найдутся по следующей формуле: xn=xn−1−md (следует понимать, что xi вычет по модулю, поэтому в этой формуле можно сменить знак, для удобства), всего решений будет d.



# **42) Алгебраические операции. Понятие группы и подгруппы, примеры**

Пусть Х – некоторое множество и введем на множестве Х бинарную алгебраическую операцию – правило, по которому каждой упорядоченной паре (x,y) X x X, где x элементов ставит в соответствие единственный элемент Z из множества X: (x,y) -> Z. Алгебраическую операцию обозначают \*. Это общее обозначение. +, х, \*, , бинарная алгебраическая операция – такая операция, которая каждой упорядоченной паре например множества G cтавит в соответствие некоторый элемент с , a\*b=c, c

Группа – непустое множество G с определенной на нем бинарной алгебраической операцией \*, обозначаем {G, \*}, эта операция обладает свойствами:   
1) Ассоциативность: (a\*b)\*c = a\*(b\*c) 2) Существует нейтральный элемент, такой что a\*e = e\*a = a 3) Для любого a существует обратный элемент , такой что

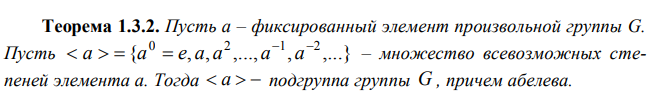
. Если соблюдается, что алгебраическая операция имеет свойство коммутативности, a\*b=b\*a, то группа является АБЕЛЕВОЙ (коммутативной). Группы с операцией умножения называются мультипликативными группами. Группы бывают конечные и бесконечные. Один из примеров группы  - множество [целых чисел](https://ru.wikipedia.org/wiki/%D0%A6%D0%B5%D0%BB%D0%BE%D0%B5_%D1%87%D0%B8%D1%81%D0%BB%D0%BE), снабжённое операцией [сложения](https://ru.wikipedia.org/wiki/%D0%A1%D0%BB%D0%BE%D0%B6%D0%B5%D0%BD%D0%B8%D0%B5): сумма любых двух целых чисел также даёт целое число, роль нейтрального элемента играет [ноль](https://ru.wikipedia.org/wiki/%D0%9D%D1%83%D0%BB%D1%8C_(%D1%87%D0%B8%D1%81%D0%BB%D0%BE)), а число с противоположным знаком является обратным элементом. Пусть имеется группа (G, \*), тогда подгруппой H G (входит в G) называется такое множество, которое является группой относительно той же алгебраической операции, что и в G. Подгруппа называется собственной, если она не совпадает с этой группой и единичным элементом. 

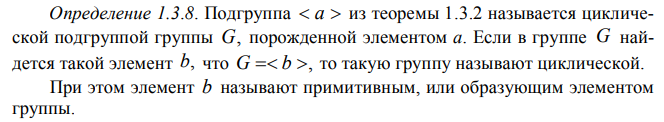
Подмножество группы G, состоящее из одного элемента 1, будет, очевидно, подгруппой, и эта подгруппа называется единичной подгруппой группы G. Сама G также является своей подгруппой. Пересечение двух подгрупп будет также подгруппой. Напр, группа четных чисел будет подгруппой группы целых чисел.

Подгруппа – подмножество в группе, которое обладает теми же свойствами, что и группа. У любой группы 2 тривиальные подгруппы: нейтральный элемент и сама группа.

# **43) Порядок элементов в группе. Циклические группы**

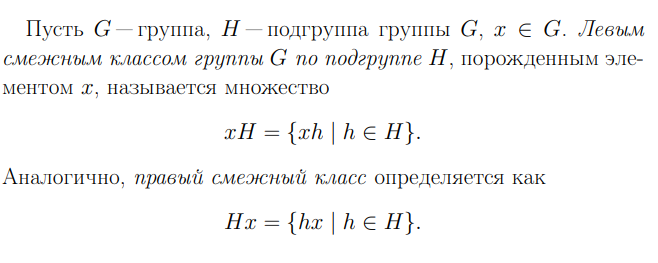
Рассмотрим фиксированный элемент данной группы G и подгруппу из всевозможных степеней целых данного элемента: a, H= a0-единичный элемент. Это множество является подгруппой. Такая подгруппа называется циклической подгруппой, порожденной данным элементом <a>. Если aan = e, тогда циклическая группа, порожденная a, конечная и имеет порядок n. Величина n – порядок элемента в данной группе. Если для всех n an ≠ e, то говорят об элементе бесконечного порядка. Порядок элемента a [группы](http://fkn.ktu10.com/?q=node/6440) G - это минимальное положительное число k, для которого справедливо равенство ak=e (где e - [единичный элемент группы](http://fkn.ktu10.com/?q=node/6609)). То есть - порядок элемента группы - это минимальная положительная степень, в которой данный элемент равен единице. Циклическая группа - [группа](https://ru.wikipedia.org/wiki/%D0%93%D1%80%D1%83%D0%BF%D0%BF%D0%B0_(%D0%BC%D0%B0%D1%82%D0%B5%D0%BC%D0%B0%D1%82%D0%B8%D0%BA%D0%B0))  (G, \*), которая может быть [порождена](https://ru.wikipedia.org/wiki/%D0%9F%D0%BE%D1%80%D0%BE%D0%B6%D0%B4%D0%B0%D1%8E%D1%89%D0%B5%D0%B5_%D0%BC%D0%BD%D0%BE%D0%B6%D0%B5%D1%81%D1%82%D0%B2%D0%BE_%D0%B3%D1%80%D1%83%D0%BF%D0%BF%D1%8B) одним элементом a, то есть все её элементы являются степенями a. Обозначение: G=<a>.





# **44) Смежные классы. Теорема Логранжа**

Пусть H – подгруппа группы G и произвольный элемент a, H<G, тогда левым смежным классом группы G по H называется множество элементов aH={ah | h. Аналогично определяется и правый смежный класс aH.



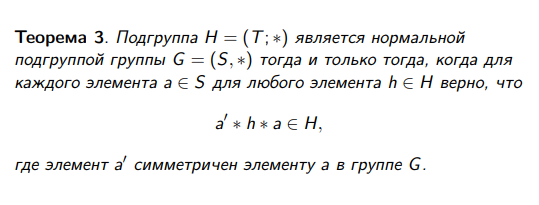
1) Теорема: Левые(правые) смежные классы G по подгруппе H либо не пересекаются, либо совпадают. 2) 2 любых элемента a и b принадлежат одному левому смежному классу, когда a-1\*b. Для правых смежных классов: a \* b-1. 3) Если H – конечная группа, то для всякого a из группы G число элементов множеств aH совпадают. 4) Группа G – всегда объединение попарно непересекающихся левых(правых) смежных классов по подгруппе H. Количество всех различных левых(правых) смежных классов группы по подгруппе называется индексом подгруппы H в группе G, обозначается G:H. Порядок конечной группы = произведению порядка и индекса любой ее подгруппы.

Теорема Логранжа: В конечных группах порядок любой подгруппы делит порядок группы. Таким образом если G конечная группа порядка n, то для любого элемента из этой группы an=e.

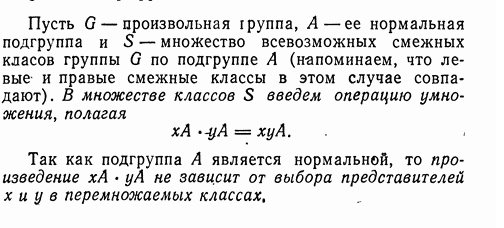
Пусть [группа](https://ru.wikipedia.org/wiki/%D0%93%D1%80%D1%83%D0%BF%D0%BF%D0%B0_(%D0%BC%D0%B0%D1%82%D0%B5%D0%BC%D0%B0%D1%82%D0%B8%D0%BA%D0%B0)) G [конечна](https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BD%D0%B5%D1%87%D0%BD%D0%B0%D1%8F_%D0%B3%D1%80%D1%83%D0%BF%D0%BF%D0%B0), и H - её [подгруппа](https://ru.wikipedia.org/wiki/%D0%9F%D0%BE%D0%B4%D0%B3%D1%80%D1%83%D0%BF%D0%BF%D0%B0). Тогда [порядок](https://ru.wikipedia.org/wiki/%D0%9F%D0%BE%D1%80%D1%8F%D0%B4%D0%BE%D0%BA_%D0%B3%D1%80%D1%83%D0%BF%D0%BF%D1%8B) G равен порядку H, умноженному на количество её левых или правых [классов смежности](https://ru.wikipedia.org/wiki/%D0%9A%D0%BB%D0%B0%D1%81%D1%81_%D1%81%D0%BC%D0%B5%D0%B6%D0%BD%D0%BE%D1%81%D1%82%D0%B8) ([индекс подгруппы](https://ru.wikipedia.org/wiki/%D0%98%D0%BD%D0%B4%D0%B5%D0%BA%D1%81_%D0%BF%D0%BE%D0%B4%D0%B3%D1%80%D1%83%D0%BF%D0%BF%D1%8B)). Количество правых и левых смежных классов любой подгруппы H в G одинаково и называется [индексом подгруппы](https://ru.wikipedia.org/wiki/%D0%98%D0%BD%D0%B4%D0%B5%D0%BA%D1%81_%D0%BF%D0%BE%D0%B4%D0%B3%D1%80%D1%83%D0%BF%D0%BF%D1%8B) H в G (обозначается G:H).

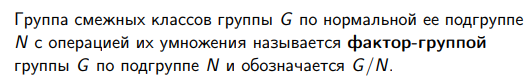
# **45) Нормальные подгруппы. Фактор группы**

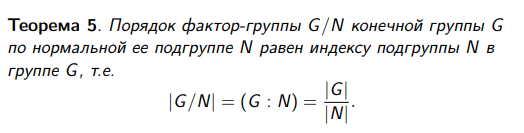
Подгруппа H группы G называется нормальной, если каждый ее правый смежный класс по подгруппе совпадает с левым смежным классом, то есть aH = Ha. Если группа коммутативна, то в ней все подгруппы нормальные.



Факторгруппа — множество [смежных классов](https://ru.wikipedia.org/wiki/%D0%93%D0%BB%D0%BE%D1%81%D1%81%D0%B0%D1%80%D0%B8%D0%B9_%D1%82%D0%B5%D0%BE%D1%80%D0%B8%D0%B8_%D0%B3%D1%80%D1%83%D0%BF%D0%BF#%D0%9A%D0%BB%D0%B0%D1%81%D1%81_%D1%81%D0%BC%D0%B5%D0%B6%D0%BD%D0%BE%D1%81%D1%82%D0%B8) [группы](https://ru.wikipedia.org/wiki/%D0%93%D1%80%D1%83%D0%BF%D0%BF%D0%B0_(%D0%BC%D0%B0%D1%82%D0%B5%D0%BC%D0%B0%D1%82%D0%B8%D0%BA%D0%B0)) по её [нормальной подгруппе](https://ru.wikipedia.org/wiki/%D0%9D%D0%BE%D1%80%D0%BC%D0%B0%D0%BB%D1%8C%D0%BD%D0%B0%D1%8F_%D0%BF%D0%BE%D0%B4%D0%B3%D1%80%D1%83%D0%BF%D0%BF%D0%B0), само являющееся группой с определённой специальным образом групповой операцией. Факторгруппа группы G по нормальной подгруппе H обычно обозначается G/H.



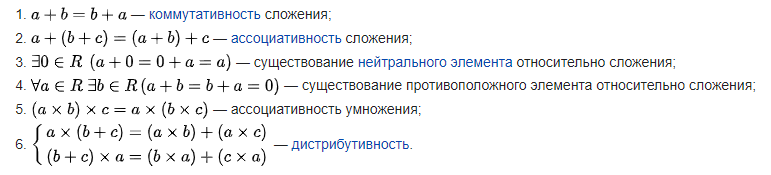




# **46) Понятие кольца и подкольца, примеры**

Кольцо — [алгебраическая структура](https://ru.wikipedia.org/wiki/%D0%90%D0%BB%D0%B3%D0%B5%D0%B1%D1%80%D0%B0%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B0%D1%8F_%D1%81%D1%82%D1%80%D1%83%D0%BA%D1%82%D1%83%D1%80%D0%B0), в которой определены операция обратимого [сложения](https://ru.wikipedia.org/wiki/%D0%A1%D0%BB%D0%BE%D0%B6%D0%B5%D0%BD%D0%B8%D0%B5) и операция [умножения](https://ru.wikipedia.org/wiki/%D0%A3%D0%BC%D0%BD%D0%BE%D0%B6%D0%B5%D0%BD%D0%B8%D0%B5) (2 бинарные операции), по свойствам похожие на соответствующие операции над [числами](https://ru.wikipedia.org/wiki/%D0%A7%D0%B8%D1%81%D0%BB%D0%BE). Простейшими примерами колец являются совокупности чисел ([целых](https://ru.wikipedia.org/wiki/%D0%A6%D0%B5%D0%BB%D0%BE%D0%B5_%D1%87%D0%B8%D1%81%D0%BB%D0%BE), [вещественных](https://ru.wikipedia.org/wiki/%D0%92%D0%B5%D1%89%D0%B5%D1%81%D1%82%D0%B2%D0%B5%D0%BD%D0%BD%D1%8B%D0%B5_%D1%87%D0%B8%D1%81%D0%BB%D0%B0), [комплексных](https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%D0%BB%D0%B5%D0%BA%D1%81%D0%BD%D1%8B%D0%B5_%D1%87%D0%B8%D1%81%D0%BB%D0%B0)), совокупности числовых [функций](https://ru.wikipedia.org/wiki/%D0%A4%D1%83%D0%BD%D0%BA%D1%86%D0%B8%D1%8F_(%D0%BC%D0%B0%D1%82%D0%B5%D0%BC%D0%B0%D1%82%D0%B8%D0%BA%D0%B0)), определённых на заданном множестве.

Обозначается K={G, +, \*}. К свойствам относятся: 1) Относительно сложения выполняется ассоциативность, коммутативность (абелева относительно сложения), существует обратный и нейтральный элемент. 2) Относительно умножения выполняется ассоциативность (ab)c = a(bc). 3) Относительно сложения и умножения выполняется дистрибутивность a(b+c) = ab+ac, (b+c)a=ab+ac.



Кольца бывают неассоциативные, с единицей и без единицы, коммутативные и некоммутативные. [Множество](https://neerc.ifmo.ru/wiki/index.php?title=%D0%9C%D0%BD%D0%BE%D0%B6%D0%B5%D1%81%D1%82%D0%B2%D0%BE&action=edit&redlink=1) A⊂R, которое определено относительно операций, определенных в кольце R, называестя подкольцом. Другими словами, A называется подкольцом в R, если оно само является кольцом относительно сужения операций, определенных на R.

При обычных операциях сложения и умножения кольцом является:

     1. Множество целых чисел.

     2. Множество рациональных чисел.

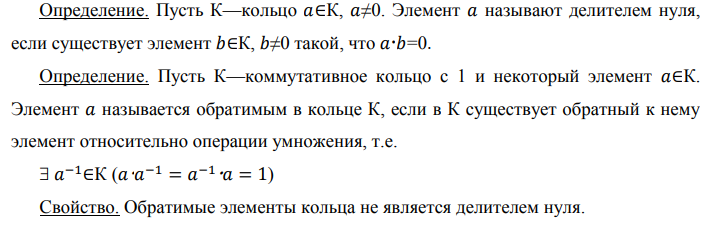
     3. Множество действительных чисел.

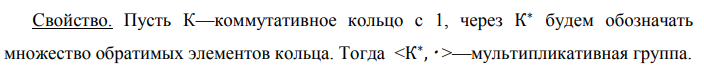
     4. Множество рациональных чисел.

Кольцо четных целых чисел является подкольцом кольца целых чисел. Кольцо целых чисел является подкольцом кольца рациональных чисел.

# **47) Мультпликативная группа кольца, делители нуля**

Если кольцо является ассоциативным кольцом с единицей, то множество обратимых элементов относительно умножения образуют группу, которую называют мультипликативной группой кольца. Если мультипликативная группа кольца = кольцу без 0, то такое множество называют телом, или алгеброй с делением. Коммутативное тело называют полем. Если в кольце 2 элемента, произведение которых = 0, их называют делителями нуля. К примеру, в кольцах целых чисел делителей 0 нет. В кольце векторов с операциями + и \* (векторное умножение) каждый отличный от 0 элемент является делителем 0.





Ненулевые элементы C:\Users\User\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\72F5518F.tmp и C:\Users\User\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\BDA3A175.tmp кольца C:\Users\User\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\D3BD084B.tmp называют делителями нуля, если C:\Users\User\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\4446D391.tmp или C:\Users\User\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\D59B2CC7.tmp.

Элемент $x\in R$ называется **левым делителем нуля**, если существует такой $y\neq 0$, что $xy=0$. Элемент $x\in R$ называется **правым делителем нуля**, если существует такой $y\neq 0$, что $yx=0$. Элемент $x\in R$ называется **делителем нуля**, если он является одновременно левым и правым делителем нуля. Если [умножение](https://math.fandom.com/ru/wiki/%D0%A3%D0%BC%D0%BD%D0%BE%D0%B6%D0%B5%D0%BD%D0%B8%D0%B5) в кольце [коммутативно](https://math.fandom.com/ru/wiki/%D0%9A%D0%BE%D0%BC%D0%BC%D1%83%D1%82%D0%B0%D1%82%D0%B8%D0%B2%D0%BD%D0%B0%D1%8F_%D0%BE%D0%BF%D0%B5%D1%80%D0%B0%D1%86%D0%B8%D1%8F), то понятия правого и левого делителя совпадают. Элемент [кольца](https://math.fandom.com/ru/wiki/%D0%9A%D0%BE%D0%BB%D1%8C%D1%86%D0%BE), который не является ни правым, ни левым делителем нуля, называется обычным элементом. Пример: в [кольце [{\displaystyle \mathbb {Z} _{6}}](https://math.fandom.com/ru/wiki/%D0%A1%D1%80%D0%B0%D0%B2%D0%BD%D0%B5%D0%BD%D0%B8%D0%B5_%D0%BF%D0%BE_%D0%BC%D0%BE%D0%B4%D1%83%D0%BB%D1%8E_%D0%BD%D0%B0%D1%82%D1%83%D1%80%D0%B0%D0%BB%D1%8C%D0%BD%D0%BE%D0%B3%D0%BE_%D1%87%D0%B8%D1%81%D0%BB%D0%B0#.D0.9A.D0.BB.D0.B0.D1.81.D1.81.D1.8B_.D0.B2.D1.8B.D1.87.D0.B5.D1.82.D0.BE.D0.B2)](https://math.fandom.com/ru/wiki/%D0%A1%D1%80%D0%B0%D0%B2%D0%BD%D0%B5%D0%BD%D0%B8%D0%B5_%D0%BF%D0%BE_%D0%BC%D0%BE%D0%B4%D1%83%D0%BB%D1%8E_%D0%BD%D0%B0%D1%82%D1%83%D1%80%D0%B0%D0%BB%D1%8C%D0%BD%D0%BE%D0%B3%D0%BE_%D1%87%D0%B8%D1%81%D0%BB%D0%B0#.D0.9A.D0.BB.D0.B0.D1.81.D1.81.D1.8B_.D0.B2.D1.8B.D1.87.D0.B5.D1.82.D0.BE.D0.B2) элементы 2, 3, 4 — делители нуля.

# **48) Идеалы колец. Кольцо полиномов**

Подкольцо G кольца K – левый идеал кольца K, если для любого k из кольца и для каждого j из подкольца jk J, то есть:

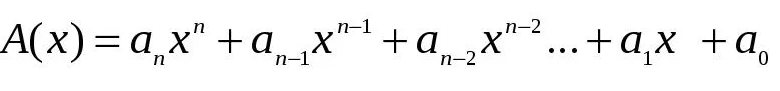
Правый идеал кольца K: .



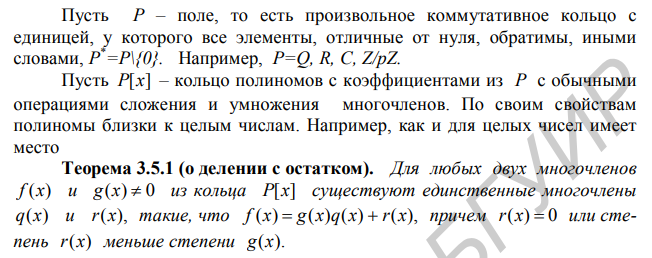
Двусторонний идеал является и правым, и левым. Отметим, что в коммутативном кольце все идеалы двусторонние. Ясно, что нулевой элемент и все кольцо являются тривиальными идеалами любого кольца. Если рассматривать множество кратных чисел, то оно образует двусторонний идеал кольца целых чисел. Для каждого элемента a кольца К множество аК является левым идеалом кольца К, он называется главным идеалом, порожденным элементом а, обозначение <а>. Кольцо, в котором каждый идеал главный, называется кольцом главного идеала. Отметим, что в поле нет собственных идеалов. Если в кольце есть делители 0, то они порождают собственные идеалы.

Множество целых чисел является кольцом главных идеалов.

Примером коммутативного кольца является множество полиномов (многочленов).

G={}

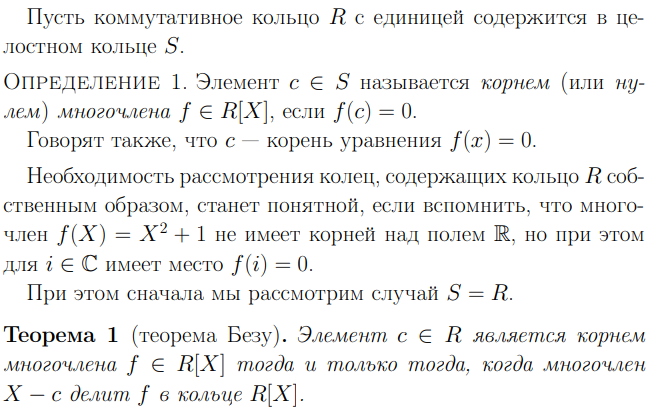
Сложение, умножение многочленов определяются обычным образом, и мы получаем коммутативное кольцо с 1. Обратимые элементы – это числа. Число x0 является корнем многочлена, если A(x0)=0.

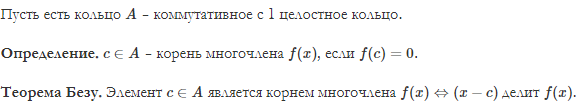


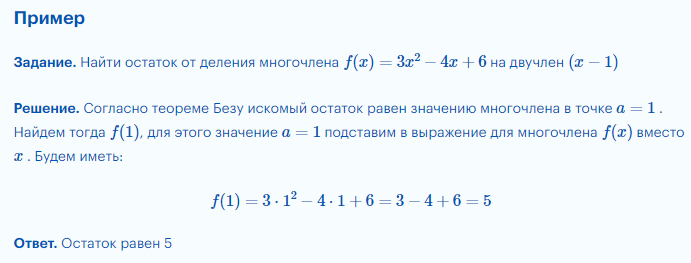
# **49) Теорема Безу и корни многочленов**

В общем случае теорема Безу звучит так: остаток от деления многочлена P(x) на двучлен (x-a) равен P(a). Отсюда также следует что множество корней многочлена P(x) тождественно множеству корней соответствующего уравнения P(x)=0.

Если в поле P существует такое натуральное n, что сумма n единичных элементов равна 0, то наименьшее n с таким свойством называется характеристикой Безу. Если для любого n сумма единичных элементов не равна 0, то говорят, что характеристика в поле равна 0.

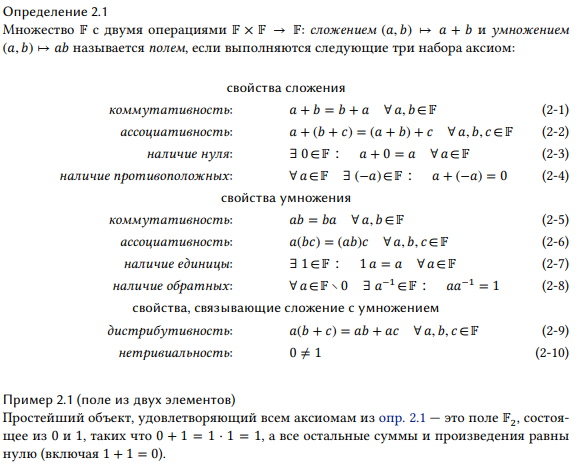






# **50) Поле. Примеры полей**

Поле — это числовая область, в которой есть четыре обычных арифметических операции: сложение, вычитание, умножение и деление, обладающие привычными свойствами соответствующих действий над рациональными числами. Обозначается P = {G, +, x}. Кольцо -> поле, если: 1) есть нейтральный элемент по x 2) выполняются все свойства кольца 3) нет делителей нуля (каждый элемент обратим, то есть нет чисел, что a x b = 0)



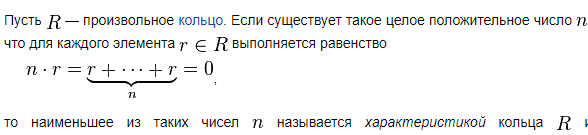
Для поля выполняются все свойства кольца (для колец нужна ассоциативность, коммутативность, обратный и нейтральный элемент по +, ассоциативность по \*, дистрибутивность по \* и +), есть нейтральный элемент по умножению, нет делителей нуля. Поле – коммутативное кольцо, где есть нейтральный элемент по умножению и для каждого элемента есть обратный. В поле нет делителей нуля. Р[ациональные](https://ru.wikipedia.org/wiki/%D0%A0%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%B0%D0%BB%D1%8C%D0%BD%D0%BE%D0%B5_%D1%87%D0%B8%D1%81%D0%BB%D0%BE), [вещественные](https://ru.wikipedia.org/wiki/%D0%92%D0%B5%D1%89%D0%B5%D1%81%D1%82%D0%B2%D0%B5%D0%BD%D0%BD%D0%BE%D0%B5_%D1%87%D0%B8%D1%81%D0%BB%D0%BE), [комплексные](https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%D0%BB%D0%B5%D0%BA%D1%81%D0%BD%D0%BE%D0%B5_%D1%87%D0%B8%D1%81%D0%BB%D0%BE) числа, [вычеты по модулю](https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BB%D1%8C%D1%86%D0%BE_%D0%B2%D1%8B%D1%87%D0%B5%D1%82%D0%BE%D0%B2) заданного [простого числа](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D1%81%D1%82%D0%BE%D0%B5_%D1%87%D0%B8%D1%81%D0%BB%D0%BE) образуют поля. Кольцо, состоящее из одного нулевого элемента (в котором 1 = 0), полем не считается.

Если Z/mZ, +, \* m – простое, то поле, а если m – составное, это будет коммутативное кольцо. Множества рациональных чисел Q и вещественных чисел R являются примерами полей, хорошо знакомых читателю из школьного курса.

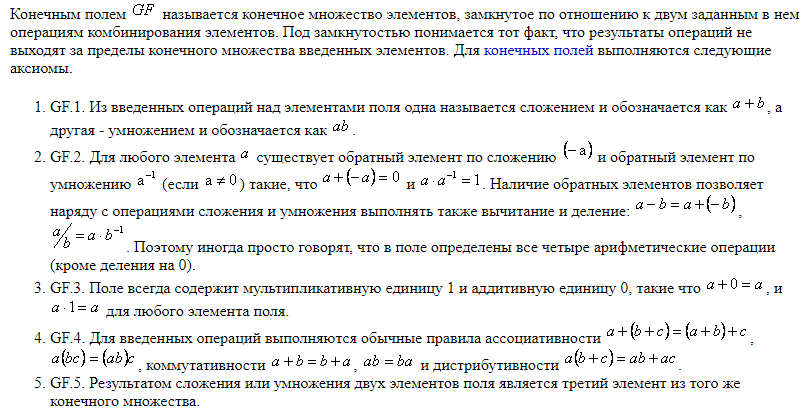
# **51) Характеристика поля. Примеры конечных полей. Поля Галуа**

Полем называется коммутативное ассоциативное кольцо с единицей, в котором любой ненулевой элемент обратим. Кольцо, состоящее из одного нулевого элемента (в котором 1 = 0), полем не считается.

Характеристикой поля P называется число 0, если na ≠ 0 для любого элемента a ≠ 0 и любого целого числа n ≠ 0 и простое число p такое, что pa = 0 для любого элемента a в противном случае.



Т.к поле — это «хорошее» кольцо, то данное определение относится и к полям: существуют поля характеристики 0 и характеристики, отличной от нуля. Характеристики [кольца целых чисел](https://dic.academic.ru/dic.nsf/ruwiki/1187190) Z, [поля рациональных чисел](https://dic.academic.ru/dic.nsf/ruwiki/1118006) Q, [поля вещественных чисел](https://dic.academic.ru/dic.nsf/ruwiki/839707) R, [поля комплексных чисел](https://dic.academic.ru/dic.nsf/ruwiki/976962) C равны нулю. Конечное поле, или поле Галуа, обозначается GF  — [поле](https://ru.wikipedia.org/wiki/%D0%9F%D0%BE%D0%BB%D0%B5_(%D0%B0%D0%BB%D0%B3%D0%B5%D0%B1%D1%80%D0%B0)), состоящее из конечного числа [элементов](https://ru.wikipedia.org/wiki/%D0%AD%D0%BB%D0%B5%D0%BC%D0%B5%D0%BD%D1%82_%D0%BC%D0%BD%D0%BE%D0%B6%D0%B5%D1%81%D1%82%D0%B2%D0%B0); это число называется порядком поля. Конечным полем называется [конечное множество](https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BD%D0%B5%D1%87%D0%BD%D0%BE%D0%B5_%D0%BC%D0%BD%D0%BE%D0%B6%D0%B5%D1%81%D1%82%D0%B2%D0%BE), на котором определены произвольные операции, называемые [сложением](https://ru.wikipedia.org/wiki/%D0%A1%D0%BB%D0%BE%D0%B6%D0%B5%D0%BD%D0%B8%D0%B5_(%D0%BC%D0%B0%D1%82%D0%B5%D0%BC%D0%B0%D1%82%D0%B8%D0%BA%D0%B0)), [умножением](https://ru.wikipedia.org/wiki/%D0%A3%D0%BC%D0%BD%D0%BE%D0%B6%D0%B5%D0%BD%D0%B8%D0%B5), [вычитанием](https://ru.wikipedia.org/wiki/%D0%92%D1%8B%D1%87%D0%B8%D1%82%D0%B0%D0%BD%D0%B8%D0%B5) и [делением](https://ru.wikipedia.org/wiki/%D0%94%D0%B5%D0%BB%D0%B5%D0%BD%D0%B8%D0%B5_(%D0%BC%D0%B0%D1%82%D0%B5%D0%BC%D0%B0%D1%82%D0%B8%D0%BA%D0%B0)), (кроме деления на 0).



Пример поле из двух элементов. Множество F2={0,1} из двух чисел «0» и «1», на котором операции сложения и умножения определены как сложение и умножение чисел с приведением результата по модулю 2. С обычной арифметикой 0+0=0, 0+1=1+0=1, 1+1=0, 0\*0=0\*1=1\*0=0, 1\*1=1. Эта логика лежит в основе двоичной системы компьютеров