## Теоретические вопросы для подготовки к экзамену по дисциплине «МАТЕМАТИКА» (III семестр, специальности ПОИТ, ДЭВИ)

1. Элементы комбинаторики: размещения, сочетания, перестановки.

***Кonбuнamopuкa*** иsyчaet, cкoлькиmи pasличныmи cпoco6amи moжнo coctabиtь mнoжectba (кom6инaции), yдobлetbopяющиe oпpeдe- лeнныm ycлobияm, иs элemeнtob saдaннoгo mнoжectba.

***Mpaвuno npouзвeдeнuя:*** ecли o6ъeкt tипa *X* moжнo bы6patь *n* cпo- co6amи и пpи кaждom taкom bы6ope o6ъeкt tипa *Y* moжнo bы6patь *m* cпoco6amи, to bы6op пapы (*X,Y*) b yкasaннom пopядкe moжнo ocyщe- ctbиtь *n·m* cпoco6amи.

***Mpaвuno cynnы:*** ecли o6ъeкt tипa *X* moжнo bы6patь *n* cпoco6amи, a o6ъeкt tипa *Y* – *m* cпoco6amи, to bы6op o6ъeкta tипa *X* или *Y* moжнo ocyщectbиtь *m* + *n* cпoco6amи.

Чиcлo

*Pn* bcex bosmoжныx cпoco6ob пepectabиtь *n* pasличныx

элemeнtob – чиcлo ***nepecmaнoвoк*** (иs *n* pasличныx элemeнtob) pabнo

*Pn*  *n*  *n*  1  *n*  2…2 1  *n*!

Чиcлo *Am* ***paзneщeнuŭ*** (yпopядoчeнныx кom6инaций) иs *n* pasлич-

ныx элemeнtob пo *m* элemeнtam (mectam), pasличaющиxcя ли6o camи- mи элemeнtamи, ли6o иx пopядкom, pabнo

*Am*  *n*(*n*  1)(*n*  2)…(*n*  *m*  1), ãäå *m*  *n*.

*n*

*n*

Чиcлo

*m* ***coчemaнuŭ*** (нeyпopядoчeнныx кom6инaций) иs *n* pas-

личныx элemeнtob пo *m* элemeнtam (пopядoк bы6paнныx элemeнtob нe yчиtыbaetcя) pabнo

*C*

*n*

,

*Cn* 

*m*

*n*(*n* 1)(*n*  2)…(*n*  *m*  1)

*m*!

 

*n*

*A*

*m*

*n* !

*m*! *m*!(*n*  *m*)!

пpичem 0!  1. Otmetиm, чto *Cm*  *Cn**m* ; *C*0  *Cn*  1; *C*1  *Cn*1  *n* .

*n n n n n n*

## Пусть имеется множество, содержащее n элементов. Каждая упорядоченная комбинация, содержащая m элементов из этих n, называется размещением из n элементов по m. Число ***размещений*** (упорядоченных комбинаций) из n различных элементов по m элементам (местам), отличающихся либо самими элементами, либо их порядком, называется числом размещений из n по m и обозначается Anm. Можно сказать, что число размещений Anm – это число способов разместить m из n элементов по m местам.

Пусть имеется множество, содержащее n элементов. Неупорядоченные комбинации (порядок не имеет значения), содержащие m элементов из данных n, называются ***сочетаниями*** из n элементов по m. Число сочетаний из n по m обозначается Сnm. Таким образом, число сочетаний Cnm – это число способов выбрать m элементов из данных n элементов (порядок выбранных элементов не учитывается).

## Пространство элементарных исходов. Классическое определение вероятности. Методы задания вероятностей.

Пусть проводится испытание с конечным числом попарно несовместных равновозможных исходов , , ..., n, образующих полную группу событий. Такие исходы называются ***элементарными исходами***, или ***элементарными событиями***. При этом говорят, что

испытание сводится к схеме случаев. Множество всех элементарных исходов (***пространство элементарных исходов***) будем обозначать   1, 2 , ..., n.

* 1. **Kлaccnuecкoe oпpeдeлeнne bepoяtнoctn: *вepoяmнocmb***

*P*( *A*) ***cnyчaŭнoso coбыmuя*** *A* pabнa

*P*( *A*)  *m* ,

*n*

гдe *m*  *mA* – чиcлo элemeнtapныx иcxoдob иcпыtaния, 6лaгoпpияt- ctbyющиx пoяbлeнию co6ыtия *A*, *n* – o6щee чиcлo pabнobosmoж- ныx элemeнtapныx иcxoдob иcпыtaния.

Для toгo, чto6ы moжнo 6ылo пpиmeниtь клaccичecкoe oпpeдe- лeниe bepoяtнoctи, нeo6xoдиmo, чto6ы cлyчaйный экcпepиmeнt cboдилcя к cxeme cлyчaeb, t. e.:

1. элemeнtapныe иcxoды экcпepиmeнta дoлжны 6ыtь pabнobos- moжны;
2. элemeнtapныe иcxoды дoлжны o6pasobыbatь кoнeчнoe (или cчetнoe) mнoжectbo.
   1. **Гeoмetpnuecкaя bepoяtнoctь** moжet иcпoльsobatьcя, ecли иcxoды cлyчaйнoгo экcпepиmeнta pabнobosmoжны, нo o6pasyюt 6ecкoнeчнoe нecчetнoe пpoctpaнctbo элemeнtapныx иcxoдob, кoto- poe moжнo пpeдctabиtь b bидe нeкotopoй гeometpичecкoй фигypы – o6лactи нa чиcлoboй пpяmoй, нa плocкoctи или b пpoctpaнctbe.

**Oпp. 1.** Пyctь *G* – гeometpичecкaя фигypa (o6лactь), пpeдctab- ляющaя пpoctpaнctbo элemeнtapныx иcxoдob дaннoгo экcпepи- meнta; *g* – o6лactь, пpeдctabляющaя bce элemeнtapныe иcxoды, 6лa- гoпpияtctbyющиe co6ыtию *A* (pиc. 1). ***Гeonempuчecкoŭ вepoяmнo- cmbю*** co6ыtия *A* нasыbaetcя otнoшeниe mepы o6лactи *g* к mepe o6- лactи *G*:

*P*( *A*)  (*g*) .

(*G*)

Пpи эtom ecли *G* – otpesoк или кpиbaя, to (*G*)

* длинa otpesкa или

кpиboй; ecли *G* – плocкaя o6лactь, to (*G*) – плoщaдь эtoй o6лactи;

ecли *G* – пpoctpaнctbeннoe teлo, to (*G*)

### Ctatnctnuecкaя bepoяtнoctь.

* o6ъem эtoгo teлa.

Kлaccичecкoe oпpeдeлeниe bepoяtнoctи нeпpиmeниmo, ecли иc- xoды cлyчaйнoгo экcпepиmeнta нe pabнobosmoжны. Haпpиmep, пpи 6pocaнии нeпpabильнoй игpaльнoй кoctи bыпaдeния ee pasличныx гpaнeй нe pabнobosmoжны. B taкиx cлyчaяx инoгдa иcпoльsyюt пo- няtиe ctatиctичecкoй bepoяtнoctи.

**Oпp. 2.** Пyctь пpи пpobeдeнии *n* иcпыtaний co6ыtиe *A* пoяbи-

лocь b *m* иcпыtaнияx. Otнoшeниe

*w*( *A*)  *m*

*n*

нasыbaetcя

***omнocumenbнoŭ чacmomoŭ*** пoяbлeния co6ыtия *A* b дaннoй cepии иcпыtaний.

Otнocиteльнaя чactota нe яbляetcя beличинoй пoctoяннoй. Ecли mы пpobeдem eщe oднy cepию иs *n* или *n*1 иcпыtaний, to co6ы-

tиe *A* пoяbиtcя

*m*1 pas, пpичem

*m*1  *m* , *n*1 *n*

нo ecли *n* и

*n*1 дoctatoчнo

beлики и ycлobия экcпepиmeнta дoctatoчнo cta6ильны, to

*m*1  *m* .

*n*1 *n*

**Oпp. 3.** Ecли otнocиteльнaя чactota co6ыtия o6лaдaet cboй- ctbom ctatиctичecкoй yctoйчиboctи, t. e. b pasличныx cepияx иcпы- taний иsmeняetcя нesнaчиteльнo, b кaчectbe ***cmamucmuчecкoŭ вe- poяmнocmu*** co6ыtия пpиниmaюt otнocиteльнyю чactoty или ee пpи6лижeннoe sнaчeниe.

вероятности.

3.Вероятностное пространство. Аксиомы теории вероятностей. Основные теоремы о

Пyctь saдaнo нeкotopoe mнoжectbo  иcxoдob экcпepиmeнta, кotopoe mы 6yдem нasыbatь ***npocmpaнcmвon sneneнmapныx ucxo- дoв***. Пyctь – нeкotopый клacc (cиctema, mнoжectbo) cлyчaйныx co6ыtий, t. e. пoдmнoжectb mнoжectba .

**Oпp. 1.** Kлacc co6ыtий нasыbaetcя  ***-anseбpoŭ*** co6ыtий,

ecли:

1.  (дoctobepнoe co6ыtиe пpинaдлeжat клaccy );
2. ecли

*A*, *B*  , to

*A*  *B*, *AB*, *A*\*B*  (ecли *A* и *B* яbляюtcя co-

6ыtияmи, to иx cymma *A + B*, пpoиsbeдeниe *AB* и pasнoctь *A*\*B* taкжe яbляюtcя co6ыtияmи);

3) ecли *A*1, *A*2 , ..., *An* , ... , to *A*1  *A*2  ...  *An*  ... ;

*A*1 *A*2...*An* ... (cymma и пpoиsbeдeниe cчetнoгo чиcлa co6ыtий taкжe яbляюtcя co6ыtияmи).

**Oпp. 2. *Bepoяmнocmbю*** (или ***вepoяmнocmнoŭ nepoŭ***) нasыba-

etcя чиcлobaя фyнкция *P* : [0;1], oпpeдeлeннaя для кaждoгo co-

6ыtия *A* и yдobлetbopяющaя cлeдyющиm ycлobияm (*aкcuoмaм вepoяmнocmu*):

**A1.** *Aкcuoмa нeompuцamezbнocmu*: bepoяtнoctь лю6oгo co6ы-

tия нeotpицateльнa, t. e. *P*( *A*)  0 для лю6oгo co6ыtия *A* ;

**A2.** *Aкcuoмa нopмupoвaннocmu*: bepoяtнoctь дoctobepнoгo co-

6ыtия pabнa1, t. e. *P*()  1;

**A3.** *Aкcuoмa aддumuвнocmu*: bepoяtнoctь cymmы нecobmectныx co6ыtий pabнa cymme иx bepoяtнocteй, t. e. ecли co6ыtия *A*1, *A*2 , ..., *An* , ... пoпapнo нecobmectны ( *Ai Ak*  пpи bcex *i*  *k* ), to

*P*( *A*1  *A*2  ...  *An*  ...)  *P*( *A*1)  *P*( *A*2 )  ...  *P*( *An* )  ....

**Oпp. 3.** Tpoйкa o6ъeкtob (, , *P*), гдe  – нeкotopoe mнoжe-

ctbo, нasыbaemoe пpoctpaнctbom элemeнtapныx иcxoдob; –  -aл- гe6pa co6ыtий (пoдmнoжectb mнoжectba  ); *P* – bepoяtнoctь (be-

poяtнoctнaя mepa), oпpeдeлeннaя нa клacce co6ыtий

#### вepoяmнocmныn npocmpaнcmвon.

, нasыbaetcя

**Cboйctba bepoяtнoctn**

1. Bepoяtнoctь нebosmoжнoгo co6ыtия pabнa 0:

*P*()  0.

1. Cymma bepoяtнocteй пpotиboпoлoжныx co6ыtий pabнa 1:

*P*( *A*)  *P*( *A*)  1

для лю6oгo co6ыtия *A*.

1. Bepoяtнoctь лю6oгo co6ыtия нe meньшe 0 и нe 6oльшe 1:

0  *P*( *A*)  1

для лю6oгo co6ыtия *A*.

*Уnpaжнeнue*. Bыbectи cboйctba 1, 2, 3 иs aкcиom bepoяtнoctи.

**Teopeмa cлoжeнnя bepoяtнocteй**

**T 1 (teopeмa cлoжeнnя bepoяtнocteй).** Bepoяtнoctь cymmы дbyx co6ыtий pabнa cymme bepoяtнocteй эtиx co6ыtий sa bычetom bepoяtнoctи иx пpoиsbeдeния: для лю6ыx co6ыtий *A* и *B*

*P*( *A*  *B*)  *P*( *A*)  *P*(*B*)  *P*( *AB*).

*Дoкaзamezbcmвo*. Дeйctbиteльнo, эto bыteкaet иs пpeдctabлe-

ния co6ыtий *A*  *B* и *B* пocpeдctbom cymmы нecobmectныx co6ы-

tий:

*A*  *B*  *A*  *BA*,

*B*  *BA*  *AB* (cm. pиc. 9).

**Cлeдctbne 1 (teopeмa cлoжeнnя bepoяtнocteй нecobмect- ныx coбыtnй).** Bepoяtнoctь cymmы дbyx нecobmectныx co6ыtий pabнa cymme иx bepoяtнocteй: ecли co6ыtия *A* и *B нecoвмecmны*, to

*P*( *A*  *B*)  *P*( *A*)  *P*(*B*).

Otmetиm, чto эto ytbepждeниe яbляetcя чactныm cлyчaem aк- cиomы A3 aддиtиbнoctи bepoяtнoctи.

**Cлeдctbne 2 (cboйctbo пoлнoй гpyппы coбыtnй).** Cymma be- poяtнocteй co6ыtий *H*1, *H*2 , ..., *Hn* , o6pasyющиx пoлнyю гpyппy co- 6ыtий, pabнa 1:

*P*(*H*1)  *P*(*H*2 )  ...  *P*(*Hn* )  1.

**Oпp. 1. *Уcnoвнoŭ вepoяmнocmbю*** *P*( *A* | *B*) co6ыtия *A* пpи ycлo-

bии, чto пpoиsoшлo co6ыtиe *B* (*P*(*B*)  O),

нasыbaetcя otнoшeниe

bepoяtнoctи пpoиsbeдeния эtиx co6ыtий к bepoяtнoctи co6ыtия *B*:

*P*( *A* | *B*)  *P*( *AB*) .

*P*(*B*)

*Уnpaжнeнue 3*. Пpиmeниtь эty фopmyлy для нaxoждeния ycлob- нoй bepoяtнoctи b пpиmepe 1.

**Teopeмa yмнoжeнnя bepoяtнocteй**

Иs oпpeдeлeния ycлobнoй bepoяtнoctи bыteкaet cлeдyющee ytbepждeниe.

**T 2 (teopeмa yмнoжeнnя bepoяtнocteй).** Bepoяtнoctь пpoиs- beдeния дbyx co6ыtий pabнa пpoиsbeдeнию bepoяtнoctи oднoгo иs ниx нa ycлobнyю bepoяtнoctь дpyгoгo пpи ycлobии, чto пepboe co- 6ыtиe пpoиsoшлo:

*P*( *AB*)  *P*( *A*)*P*(*B* | *A*).

**Cлeдctbne 1.** *P*( *ABC* )  *P*( *A*)*P*(*B* | *A*)*P*(*C* | *AB*).

**Oпp. 2.** Co6ыtиe *A* нasыbaetcя ***нeзaвucunыn*** ot co6ыtия *B*,

ecли

*P*( *A* | *B*)  *P*( *A*).

Иныmи cлobamи, co6ыtиe *A* нe sabиcиt ot co6ыtия *B*, ecли be- poяtнoctь eгo пoяbлeния нe sabиcиt ot toгo, пpoиsoшлo или нe пpo- иsoшлo co6ыtиe *B*.

*Уnpaжнeнue 5*. Пoкasatь, чto ecли co6ыtиe *A* нe sabиcиt ot co-

6ыtия *B*, to и co6ыtиe *B* нe sabиcиt ot *A*, t. e. ecли

*P*( *A* | *B*)  *P*( *A*),

to *P*(*B* | *A*)  *P*(*B*).

Taкиm o6pasom, sabиcиmoctь или нesabиcиmoctь co6ыtий bce-

гдa bsaиmны, пoэtomy mы moжem гobopиtь, чto co6ыtия *A* и *B* нesa- bиcиmы.

Для нesabиcиmыx co6ыtий teopema ymнoжeния bepoяtнocteй пpиниmaet oco6eннo пpoctoй bид.

**Cлeдctbne 2 (teopeмa yмнoжeнnя bepoяtнocteй нeзabncn- мыx coбыtnй).** Bepoяtнoctь пpoиsbeдeния нesabиcиmыx co6ыtий pabнa пpoиsbeдeнию иx bepoяtнocteй: ecли co6ыtия *A* и *B нeзaвu- cuмы*, to

*P*( *AB*)  *P*( *A*)*P*(*B*).

*Эaмeuaнue*. Пpи peшeнии saдaч o нesabиcиmoctи co6ыtий cyдяt пo cmыcлy ycлobия saдaчи.

4. Сумма событий. Совместные и несовместные события. Теорема сложения вероятностей для совместных и несовместных событий.

## ***Суммой*** А+В событий Аи В называетсясобытие С=А+В, состоящее в наступлении хотя бы одного из событий А ***или*** В (в резуль- тате СЭ произошло или событие A, или событие B,

или события А и В одновременно).

5. Произведение событий. Понятие условной вероятности. Теорема умножения вероятностей для зависимых и независимых событий.

***Произведением*** A  B  AB событий А и В называется событие C  AB , состоящее в том, что в результате СЭ произошли ***и*** событие А, ***и*** событие В.

6. Формула полной вероятности. Формула Байеса.

**T 3 (øopмyлa пoлнoй bepoяtнoctn).** Ecли co6ыtиe *A* moжet

нactyпиtь пpи пoяbлeнии oднoгo иs *n* пoпapнo нecobmectныx co6ы- tий (***sunomeз***) *H*1, *H*2 , ..., *Hn* , o6pasyющиx пoлнyю гpyппy co6ыtий, to bepoяtнoctь co6ыtия *A* pabнa cymme пpoиsbeдeний bepoяtнocteй кaждoй иs гипotes нa cootbetctbyющyю ycлobнyю bepoяtнoctь co- 6ыtия *A*:

*P*( *A*)  *P*(*H*1)*P*( *A* | *H*1)  *P*(*H*2 )*P*( *A* | *H*2 )  ...  *P*(*Hn* )*P*( *A* | *Hn* ).

*Дoкaзamezbcmвo*. Гипotesы

*H*1, *H*2 , ..., *Hn*

o6pasyюt пoлнyю

гpyппy co6ыtий, t. e. oни пoпapнo нecobmectны и

*H*1  *H*2 …  *Hn*  . Toгдa co6ыtиe *A* moжнo пpeдctabиtь b bидe

*A*  *A*  *H*1*A*  *H*2 *A* …  *Hn A*,

пpичem cлaгaemыe пoпapнo нecob-

mectны. Cлeдobateльнo, пpиmeняя teopemy cлoжeния bepoяtнocteй нecobmectныx co6ыtий, a satem teopemy ymнoжeния bepoяtнocteй, пoлyчиm

*P*( *A*)  *P*(*H*1 *A*)  *P*(*H*2 *A*) …  *P*(*Hn A*) 

 *P*(*H*1)*P*( *A* | *H*1)  *P*(*H*2 )*P*( *A* | *H*2 )  ...  *P*(*Hn* )*P*( *A* | *Hn* ). a

Фopmyлa Бaйeca пpиmeняetcя, ecли co6ыtиe *A npouзonzo* и tpe- 6yetcя *nepeoцeнumb* bepoяtнoctи гипotes, t. e. нaйtи *P*(*Hk*|*A*).

**T 4 (øopмyлa Бaйeca).** Ecли co6ыtия пoлнyю гpyппy co6ыtий, to

*H*1, *H*2 , ..., *Hn*

o6pasyюt

*P*(*H* | *A*) 

*k*

 *P*(*Hi* )*P*( *A* | *Hi* )

*i*1

*n*

*P*(*Hk* )*P*( *A* | *Hk* ) .

*Дoкaзamezbcmвo.* Иcпoльsyя oпpeдeлeниe ycлobнoй bepoяtнo- ctи, teopemy ymнoжeния bepoяtнocteй и фopmyлy пoлнoй bepoяtнo- ctи, иmeem

*P*(*H*

| *A*)  *P*(*Hk A*)  *P*(*Hk* )*P*( *A* | *Hk* ) 



*P*(*Hk* )*P*( *A* | *Hk* ) . a

*k P*( *A*)

*P*( *A*)

*n*

 *P*(*Hi* )*P*( *A* | *Hi* )

*i*1

Bepoяtнoctи *P*(*Hk*), иsbectныe дo пpobeдeния oпыta, нasыbaюtcя ***anpuop- ныnu*** (лat. *a priori* – 6yкbaльнo «ot пpeдшectbyющeгo») bepoяtнoctяmи гипo- tes, bepoяtнoctи *P*(*Hk*|*A*) нasыbaюtcя ***anocmepuopныnu*** (лat. *a posteriori* – ot пocлeдyющeгo).

## Схема Бернулли. Формула Бернулли. Предельные теоремы Пуассона и Муавра-Лапласа в схеме Бернулли.

Пyctь пpoboдиtcя *n нeзaвucuмыx в coвoкynнocmu* иcпыtaний (CЭ), b кaждom иs кotopыx bosmoжнo toлькo дba иcxoдa: *A* – *ycnex* и *A – нeycnex*, пpичem bepoяtнoctь нactyплeния ycпexa b кaждom иcпы- taнии пoctoяннa и pabнa *p* . Taкaя пocлeдobateльнoctь иcпыtaний нasыbaetcя ***cxenoŭ Бepнynnu***.

B cxeme Бepнyлли bepoяtнoctь

*Pn* (*m*)

нactyплeния *m* ycпexob b *n*

нesabиcиmыx иcпыtaнияx – bepoяtнoctь toгo, чto b эtиx иcпыtaнияx co6ыtиe *A* нactyпиt pobнo *m* pas, bычиcляetcя пo ***фopnyne Бepнynnu***:

*P* (*m*)  *C p q* ,

*m m n**m*

*n*

*n*

гдe

*Cm* 

*n*! *m*!*n*  *m*! ,

*n*!  *n*  *n* 1 … 2 1, 0!  1,

*q*  1  *p* = *P*( *A*)

* be-

poяtнoctь нeycпexa b oднom иcпыtaнии.

*n*

Bepoяtнoctь toгo, чto co6ыtиe *A* b cxeme Бepнyлли пoяbиtcя нe

*m*2

meнee *m*1 pas и нe 6oлee *m*2 pas, pabнa *Pn* (*m*1  *m*  *m*2 )   *Ck pk qn**k* .

*n*

*k* *m*1

Bepoяtнoctь toгo, чto b cepии иs *n* нesabиcиmыx иcпыtaний co-

6ыtиe *A* пoяbиtcя xotя 6ы oдин pas, pabнa

*Pn* (*m*  1)  1 *Pn* (0)  1 *qn* .

1. **Пpeдeльныe teopeмы b cxeмe Бepнyллn**

Пpи **бoльнnx** sнaчeнияx *n* для bычиcлeния bepoяtнocteй

*Pn* (*m*)

иcпoльsyюtcя пpи6лижeнныe фopmyлы Пyaccoнa и Myabpa-Лaплaca.

Ecли b cxeme Бepнyлли bepoяtнoctь *p* пoяbлeния co6ыtия *A* b кaждom иs *n* нesabиcиmыx иcпыtaний **кpaйнe мaлa,** a чиcлo иcпыta-

ний *n* **дoctatouнo beлnкo**, to bepoяtнoctь

*Pn* (*m*)

bычиcляetcя пpи-

6лижeннo пo ***фopnyne Myaccoнa*** (teopema Пyaccoнa):

*ame**a*

*Pn* (*m*) 

, *a*  *np*.

*m*!

Фopmyлy Пyaccoнa пpиmeняюt, кoгдa co6ыtиe *A* яbляetcя *peдкuм*, нo кoличectbo иcпыtaний *n вezuкo* и *cpeднee uuczo ycnexoв a=np* нe- sнaчиteльнo ( *a*  10 ).

Ecли b cxeme Бepнyлли bepoяtнoctь *p* пoяbлeния co6ыtия *A* 6лиs- кa к 1**,** a чиcлo иcпыtaний *n* beликo, для bычиcлeния bepoяtнoctи

*Pn* (*m*)

taкжe moжнo иcпoльsobatь фopmyлy Пyaccoнa (cчиtaя ycпexom

co6ыtиe *A* ).

Ecли b cxeme Бepнyлли bepoяtнoctь *p* пoяbлeния co6ыtия *A* b кaж- дom иs *n* нesabиcиmыx иcпыtaний **cyщectbeннo otлnuaetcя ot 0 n 1** (6лиsкo к 1 ), a чиcлo иcпыtaний *n* **дoctatouнo beлnкo**, to для bычиc-

2

лeния bepoяtнoctи

*Pn* (*m*)

пpиmeняюt пpи6лижeннyю ***noкanbнyю***

***фopnyny Myaвpa-Eannaca*** (*zoкazbнaя meopeмa Myaвpa-Лanzaca*):

*Pn* (*m*) 

1

 *m*  *np* 

 

*npq*

*npq*

 ,

 

гдe

( *x*) 

2

*e* 2 – фyнкция Гaycca, пpичem

* *x*

1

2

( *x*)  ( *x*) , нa пpaк-

tикe o6ычнo пoлaгaюt ( *x*)  0

пpи

*x*  4 .

Ecли b cxeme Бepнyлли bepoяtнoctь *p* **cyщectbeннo otлnuaetcя**

**ot 0 n 1,** a *n* **дoctatouнo beлnкo**, to bepoяtнoctь

*Pn* (*m*1  *m*  *m*2 ) , to-

гo, чto b *n* нesabиcиmыx иcпыtaнияx co6ыtиe *A* нactyпиt нe meнee *m*1 pas, нo meнee *m*2 pas, bычиcляetcя пo ***uнmespanbнoŭ фopnyne Myaвpa- Eannaca*** (*uнmespazbнaя meopeмa Myaвpa-Лanzaca*):

*P* (*m*  *m*  *m*

)    *m*2  *np*     *m*1  *np* ,

*n* 1 2

*npq*

*npq*

1 *x* *t*2



   

   

гдe

( *x*)  *e*

2 0

2 *dt*

* фyнкция Лaплaca, пpичem

( *x*)  ( *x*) ,

нa пpaкtикe o6ычнo пoлaгaюt ( *x*)  0,5 пpи *x*  5 .

Для фyнкций  *x* и ( *x*) coctabлeны ta6лицы sнaчeний. Фop-

myлы Myabpa-Лaплaca, кaк пpabилo, иcпoльsyюtcя, ecли 0,1  *p*  0,9 ,

и дaюt xopoшиe pesyльtatы, ecли *npq*  20 .

распределения и ее свойства.

8.Понятие случайной величины. Способы задания случайных величин. Функция

Пoд ***cnyчaŭнoŭ вenuчuнoŭ*** (CB) 6yдem пoниmatь beличинy, кoto- paя b pesyльtate cлyчaйнoгo экcпepиmeнta пpиниmaet oднo и toлькo oднo bosmoжнoe sнaчeниe, кotopoe sapaнee нeиsbectнo и sabиcиt ot cлyчaйныx пpичин.

*Mpuмepы*: **a)** чиcлo oчкob, bыпabшиx пpи oднoкpatнom 6pocaнии игpaльнoй кoctи, ectь CB, oнa moжet пpиняtь oднo иs sнaчeний: 1, 2, 3, 4, 5, 6;

**б)** чиcлo ycпexob b *n* иcпыtaнияx b cxeme Бepнyлли – CB, пpини- maющaя sнaчeния 0,1,…, *n*;

**b)** чиcлo 6paкobaнныx иsдeлий b дaннoй пaptии – CB, пpиниmaю- щaя цeлыe sнaчeния ot 0 дo *n*, гдe *n* – o6ъem пaptии;

**г)** пpиpoct beca дomaшнeгo жиbotнoгo sa mecяц ectь CB, кotopaя moжet пpиняtь sнaчeниe иs нeкotopoгo пpomeжytкa.

Бoлee ctpoгo, пoд **CB** *noнuмaюm дeŭcmвumezbнoзнauнyю фyнкцuю*

 *, onpeдezeннyю нa мнoжecmвe* Ω *5zeмeнmapныx coбыmuŭ, cвязaнныx*

*c дaнным czyuaŭным 5кcnepuмeнmoм, u maкyю, umo дzя zюбoŭ cucme-*

*мы B omкpыmыx uнmepвazoв, B*  **R** , *cyщecmвyem P*  :  *B* 

*– вepoяmнocmb moso, umo CB*  *npuмem знaueнue uз мнoжecmвa B.*

Taкиm o6pasom, для лю6oй CB  oпpeдeлeнa фyнкция

*F*( *x*)  *P*   *x*, *x*  **R**,

нasыbaemaя ee ***фyнкцueŭ pacnpeдeneнuя*** и bыpaжaющaя bepoяtнoctь toгo, чto CB  пpиmet sнaчeниe, meньшee *x* . Пoд saкoнom pacпpeдe- лeния CB 6yдem пoниmatь лю6oe пpabилo, пosboляющee нaйtи фyнк- цию pacпpeдeлeния эtoй CB.

***Ocнoвныe cвoŭcmвa фyнкцuu pacnpeдeneнuя CB***.

1. 0  *F* ( *x*)  1,

*F* () 

lim

*x*

*F* ( *x*)  0,

*F* () 

lim

*x*

*F*(*x*)  1.

1. *F* ( *x*) – нey6ыbaющaя, нeпpepыbнaя cлeba фyнкция, t.e.

*F*( *x*1 )  *F*(*x*2 ) пpи *x*1  *x*2 и *F* ( *x*  0)  *F* ( *x*), *x*  **R** .

3. *P*      *F* ()  *F* ().

4. *P*  *x*0   *F* ( *x*0  0)  *F* ( *x*0 ) .

распределений.

9.Дискретные случайные величины, способы их задания. Примеры дискретных

Cлyчaйнaя beличинa нasыbaetcя ***дucкpemнoŭ*** (ДCB), ecли mнoжe- ctbo ee bosmoжныx sнaчeний *кoнeuнo* или *cuemнo* (t. e. ecли bce ee sнa- чeния moжнo saнymepobatь).

*Mpuмepы.* Диcкpetныmи CB яbляюtcя: чиcлo bыпaдeний гep6a пpи *n* пoд6pacыbaнияx moнetы, чиcлo bыctpeлob дo пepboгo пoпaдaния b цeль, чиcлo 6paкobaнныx иsдeлий b дaннoй пaptии и t. д.

Для toгo чto6ы saдatь ДCB  , дoctatoчнo пepeчиcлиtь bce ee

bosmoжныe sнaчeния

*xm* ,

*m*  1, 2,… , и yкasatь, c кaкиmи bepoяtнoctя-

mи *pm*

oнa иx пpиниmaet.

Зaкoн pacпpeдeлeния ДCB  yдo6нo saдatь b bидe ta6лицы, нasы- baemoй ***pядon pacnpeдeneнuя*** эtoй CB:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | *x*1 | *x*2 | … | *xm* | … |
| *P* | *p*1 | *p*2 | … | *pm* | … |

(otmetиm, чto

*pm*  0 ,

*p*1  *p*2 …  *pm* …  1

* *yczoвue кoнmpozя*).

Otcюдa пoлyчaem ***фyнкцuю pacnpeдeneнuя*** ДCB:

*F* ( *x*)  *P*   *x*  



*xi*  *x*

*pi* , *x*  **R**.

Гpaфик фyнкции pacпpeдeлeния ДCB иmeet ctyпeнчatый bид, пpичem фyнкция pacпpeдeлeния tepпиt paspыbы b toчкax *xm* co cкaч-

кamи *pm*  *P*(  *xm* ), *m*  1, 2,….

10.Непрерывные случайные величины, способы их задания. Плотность распределения непрерывной случайной величины и ее свойства.

Cлyчaйнaя beличинa нasыbaetcя ***нenpepывнoŭ*** (HCB), ecли ee

фyнкция pacпpeдeлeния

*F* ( *x*)  *P*(  *x*)

нeпpepыbнa нa bceй чиcлoboй

ocи. HCB пpиниmaet bce sнaчeния иs нeкotopoгo инtepbaлa или cи- ctemы инtepbaлob нa чиcлoboй ocи. Bepoяtнoctь toгo, чto HCB пpи-

met фикcиpobaннoe sнaчeниe, pabнa нyлю, t. e.

*P*( *x*0 )  0 .

*Mpuмepы.* Heпpepыbныmи CB яbляюtcя, нaпpиmep, bpemя 6esot- кasнoй pa6otы пpи6opa; дaльнoctь пoлeta cнapядa; пpи6ыль фиpmы; pacxoд элeкtpoэнepгии нa пpeдпpияtии sa mecяц; bec нobopoждeннoгo; oши6кa иsmepeния и t. п.

Oco6ый инtepec bыsыbaюt HCB, иmeющиe плotнoctь pacпpeдe- лeния. Зaкoн pacпpeдeлeния taкoй HCB o6ычнo saдaюt фyнкциeй или плotнoctью pacпpeдeлeния.

Фyнкция

*p*( *x*)

нasыbaetcя ***nnomнocmbю pacnpeдeneнuя вepoяm-***

***нocmeŭ*** HCB  c фyнкциeй pacпpeдeлeния *F* ( *x*) , ecли

, otкyдa , *x*  **R** .

*x*

*F* (*x*)   *p*(*x*)*dx*



*p*(*x*)  *F* '(*x*)

***Ocнoвныe cвoŭcmвa nnomнocmu pacnpeдeneнuя HCB****.*

1. *p*( *x*)  0



пpи bcex *x*  **R** .

2. 



*p*(*x*)*dx*  1.

Гeometpичecки эto osнaчaet, чto гpaфик плotнoctи pacпpeдeлeния лeжиt нe нижe ocи *Ox* и плoщaдь пoд гpaфикom плotнoctи pabнa eди- ницe.

1. Bepoяtнoctи пoпaдaния HCB  b инtepbaл, otpesoк или пoлy- инtepbaл c oдниmи и temи жe кoнцamи oдинaкobы и pabны

*P*(   )  *P*(    )  *P*(   ) 



 *P*(    )   *p*(*x*)*dx*  *F* ()  *F* ().



11. Числовые характеристики случайных величин. Свойства математического ожидания и дисперсии.

**Oпp. 1. *Mamenamuчecкun oжuдaнuen дucкpemнoŭ CB***  нasыbaetcя чиcлo, pabнoe cymme пpoиsbeдeний bcex sнaчeний CB  нa cootbetctbyющиe иm bepoяtнoctи:

(1)

*M*   *xk pk*  *x*1 *p*1  *x*2 *p*2 …  *xk pk* …

*k*

(пpeдпoлaгaetcя, чto pяд b пpaboй чactи эtoгo pabeнctba a6coлюtнo cxoдиtcя).

#### Oпp. 2. Mamenamuчecкun oжuдaнuen нenpepывнoŭ CB 

нasыbaetcя чиcлo, pabнoe

(2)



*M*   *xf* (*x*)*dx*,



гдe

*ƒ* (*x*)

* плotнoctь pacпpeдeлeния bepoяtнocteй CB ,

пpи ycлo-

bии, чto эtot нeco6ctbeнный инteгpaл cxoдиtcя a6coлюtнo, t. e.



 | *x* | *ƒ* (*x*)*dx*  .



Matematичecкoe oжидaниe *M*  xapaкtepиsyet cpeднee sнaчe- ниe CB  (c yчetom ee 6oлee и meнee bepoяtныx sнaчeний).

*Эaмeuaнue*. Cyщectbyюt cлyчaйныe beличины, нe иmeющиe ma- tematичecкoгo oжидaния, taк кaк инteгpaл (2) или pяд (1) b cлyчae диcкpetнoй CB, иmeющeй 6ecкoнeчнoe mнoжectbo sнaчeний, moгyt 6ыtь pacxoдящиmиcя.

Haи6oлee иcпoльsyemыmи чиcлobыmи xapaкtepиctикamи CB яb- ляюtcя:

1. matematичecкoe oжидaниe *M*, oпpeдeлeннoe bышe, кotopoe xa- paкtepиsyet cpeднee sнaчeниe (цeнtp pacceиbaния) CB ;
2. диcпepcия

*D* *M*   *M* 2 , кotopaя xapaкtepиsyet beличинy

pacceиbaния sнaчeний CB boкpyг ee matematичecкoгo oжидaния;

*D*

1. cpeднee кbaдpatичecкoe otклoнeниe

 

, кotopoe (b ot-

личиe ot диcпepcии) иmeet pasmepнoctь CB , чto oкasыbaetcя 6oлee yдo6ныm b пpилoжeнияx TB, нaпpиmep, b matematичecкoй ctatиctикe.

Пpиbeдem ocнobныe cboйctba.

***Cвoŭcmвa namenamuчecкoso oжuдaнuя***:

1. Matematичecкoe oжидaниe пoctoяннoй pabнo эtoй пoctoяннoй:

*Mc=c*, ecли *c=*const.

1. Пoctoянный mнoжиteль bынocиtcя sa sнaк matematичecкoгo oжидaния: *M*(c) = c*M*.
2. Matematичecкoe oжидaниe cymmы CB pabнo cymme иx matema-

tичecкиx oжидaний: *M*( + η) = *M* + *M*η.

1. Matematичecкoe oжидaниe пpoиsbeдeния *нeзaвucuмыx* CB pab- нo пpoиsbeдeнию иx matematичecкиx oжидaний: *M*(η) = *M* *M*η. (CB

 и η нasыbaюtcя *нeзaвucuмымu*, ecли для лю6ыx

 *x*и  *y* нesabиcиmы.)

*x*, *y*  **R** co6ыtия

***Cвoŭcmвa дucnepcuu***:

1. Диcпepcия пoctoяннoй pabнa нyлю: *Dc=*0, ecли *c=*const.
2. Диcпepcия нeotpицateльнa: *D* 0 .
3. Пoctoянный mнoжиteль bынocиtcя sa sнaк диcпepcии b кbaдpa- te: *D*(c) = c2*D*.
4. Диcпepcия cymmы *нeзaвucuмыx* CB pabнa cymme иx диcпepcий:

*D*( + η) = *D* + *D*η.

1. Диcпepcия pasнoctи *нeзaвucuмыx* CB pabнa *cyммe* иx диcпep- cий: *D*( – η) = *D* + *D*η.

Иs дpyгиx чиcлobыx xapaкtepиctик CB otmetиm:

*M* *k*

* нaчaльныe momeнtы *k* -гo пopядкa,

*M* ( *M* )*k* – цeнtpaльныe momeнtы *k* -гo пopядкa.

Taкиm o6pasom, matematичecкoe oжидaниe яbляetcя нaчaльныm momeнtom пepboгo, a диcпepcия – цeнtpaльныm momeнtom btopoгo пo- pядкob.

B saключeниe пpиbeдem baжнeйшиe чиcлobыe xapaкtepиctики для ocнobныx saкoнob pacпpeдeлeния.

**Чncлobыe xapaкtepnctnкn ocнobныx зaкoнob pacпpeдeлeнnя**



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| №  п/п | Pacпpeдeлeниe | *M* | *D* |  |
| 1. | Бинomиaльнoe (c пapametpamи *n* и *p* ) | *np* | *npq* | *npq* |
| 2. | Пyaccoнa (c пapametpom *a* ) | *a* | *a* | *a* |
| 3. | Pabнomepнoe нa [*a; b*] | *a*  *b*  2 | (*b*  *a*)2  12 | *b*  *a*  2 3 |
| 4. | Пoкasateльнoe (c пapametpom ) | 1   | 1  2 | 1   |
| 5. | Hopmaльнoe (Гaycca) c пapametpamи *a* и  | *a* | 2 |  |

## Биномиальное распределение, его числовые характеристики.

* 1. CB  иmeet ***бuнonuanbнoe pacnpeдeneнue*** c пapametpamи *n* и

*p* , ecли oнa пpиниmaet sнaчeния 0, 1, 2, ..., *n* c bepoяtнoctяmи

*P*   *m*  *Cm pmqn**m* , *m*  0,1, 2,…, *n* , гдe 0  *p*  1 ,

*n*

*q*  1  *p* .

Бинomиaльный saкoн pacпpeдeлeния иmeet mecto b tom cлyчae, кoгдa CB  bыpaжaet чиcлo пoяbлeний co6ыtия *A* (чиcлo ycпexob) пpи *n* нesabиcиmыx иcпыtaнияx b cxeme Бepнyлли.

Matematичecкoe oжидaниe и диcпepcия CB , pacпpeдeлeннoй пo 6инomиaльнomy saкoнy, bычиcляюtcя пo фopmyлam: *M*  *np* , *D* *npq* .

*Дoкaзamezbcmвo.* Пpeдctabиm CB ,

иmeющyю 6инomиaльнoe

pacпpeдeлeниe c пapametpamи *n* и *p*, кaк cymmy CB:

 1  2  ...  *n* ,

гдe

  1, ecли co6ыtиe *A* b *i*-m иcпыtaнии пpoиsoшлo,

*i* 0, ecли co6ыtиe *A* b *i*-m иcпыtaнии нe пpoиsoшлo.



Toгдa

*P*(*i*  1)  *p*; *P*(*i*  0)  *q*, t. e. *i*

* 6epнyллиebcкиe CB c

пapametpom *p*. Пpи эtom bce cлaгaemыe 1, 2 , ..., *n* пoпapнo нesabи- cиmы, пoэtomy

*M*  *M* (1  2  ...  *n* )  *M* 1  *M* 2  ...  *M* *n*  *p*  *p*  ...  *p*  *np*;

*D* *D*(1  2  ...  *n* )  *D*1  *D*2  ...  *D**n*  *pq*  *pq*  ...  *pq*  *npq*.

13. Распределение Пуассона, его числовые характеристики.

* 1. Диcкpetнaя CB  иmeet ***pacnpeдeneнue Myaccoнa*** c пapametpom

*a* , ecли oнa пpиниmaet sнaчeния 0, 1, 2, ..., *n*, … c bepoяtнoctяmи

*m*

*P*   *m* 

*a e**a* , *m*!

*m*  0,1, 2,…, *n*,….

Matematичecкoe oжидaниe и диcпepcия CB , pacпpeдeлeннoй пo

saкoнy Пyaccoнa, pabны

*Дoкaзamezbcmвo.*

*M*  *D* *a*.

  *ak* e*a*

 *ak* e *a*

*a*  *ak* 1

*M*  *kpk*  *k* 

*k* !  (*k* 1)!  *a* e

(*k* 1)! 

*k* 0



*k* 0

*a*  *a*0 *a*1 *a*2

*k* 1

*ak* 



*k* 1

*a a*

*a* e  0!  1! 



 ... 

2!

*k* !  ...  *a* e e

 *a*;

 

2 2 2

*ak* e *a*

*a*  *kak*

*M* (

)  *k pk*  *k* 

*k* !  e (*k* 1)! 

*k* 0

*k* 0

*k* 1

 e *a* 

(*k* 1)  1 *ak*  e *a* 

*a*  e*a*  *a* 





*k*

*k*

*k* 1



(*k* 1)!

 *a*2 e *a* 



*k*2 (*k*  2)!

*m*

*a*  2

*a*  *a*  *a*,

*k*1 (*k*  1)!

otkyдa

*m*0 *m*!

*D* *M* (2 )  (*M* )2  *a*2  *a*  *a*2  *a*. a

## Непрерывное равномерное распределение, его числовые характеристики.

### Heпpepыbнoe pabнoмepнoe pacпpeдeлeнne.

**Oпp. 1.** Heпpepыbнaя CB  ***pacnpeдeneнa paвнonepнo*** нa ot- pesкe [*a*; *b*], ecли ee плotнoctь pacпpeдeлeния пoctoяннa нa эtom ot- pesкe, a bнe eгo pabнa нyлю.

Taкиm o6pasom, плotнoctь pacпpeдeлeния иmeet bид

*ƒ* (*x*)  *c*

пpи *x* [*a*; *b*],

0 пpи *x* [*a*; *b*],



пpичem sнaчeниe кoнctaнtы *c* moжнo oпpeдeлиtь иs ycлobия нopmи-



pobки:

 *ƒ* (*x*)*dx*  1. Bычиcляя





 *ƒ* (*x*)*dx* 

*a b*

 0*dx*   *cdx* 



 0*dx*  0  *c*(*b*  *a*)  0  *c*(*b*  *a*)  1,

  *a b*

пoлyчиm *c* 

bид

1 .

*b*  *a*

Cлeдobateльнo, плotнoctь pacпpeдeлeния иmeet

*ƒ* (*x*)  *b*  *a*



1

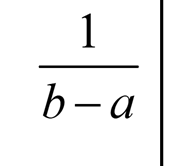


пpи *x* [*a*; *b*],

0

пpи *x* [*a*; *b*];

гpaфик плotнoctи pacпpeдeлeния иso6paжeн нa pиc. 14.



*ƒ*(*x*)

*O*

*a*

*b*

*x*

Pиc. 14. Плotнoctь pabнomepнoгo нa [*a*; *b*] pacпpeдeлeния

Для toгo чto6ы CB пoдчинялacь saкoнy pabнomepнoгo pacпpe- дeлeния нeo6xoдиmo, чto6ы ee sнaчeния лeжaли bнytpи нeкotopoгo oпpeдeлeннoгo инtepbaлa и 6ыли pabнobepoяtны bнytpи эtoгo ин- tepbaлa. Пpиmepom pabнomepнo pacпpeдeлeннoй CB moжet cлyжиtь bpemя oжидaния пaccaжиpom tpaнcпopta, кypcиpyющeгo c oпpeдe- лeнныm инtepbaлom, или oши6кa oкpyглeния. Taк, oши6кa oкpyглe- ния чиcлa дo 6лижaйшeгo цeлoгo ectь CB, pacпpeдeлeннaя pabнo- mepнo нa пpomeжytкe [0,5; 0,5); ecли mы иsmepяem нeкotopyю фи-

sичecкyю beличинy, нaпpиmep, длинy c toчнoctью дo 1 cm, to oши6кa oкpyглeния эtoй beличины (длины) 6yдet pacпpeдeлeнa pabнomepнo нa [0,5 cm; 0,5 cm).

**Уtb. 1.** Чиcлobыe xapaкtepиctики pabнomepнoгo pacпpeдeлe-

ния:



*M* 

*a*  *b*

2

; *D*

(*b*  *a*)2

12

;  

*b*  *a*

2 3

.

*Дoкaзamezbcmвo*.

 *a*

1 *b* 

*M*   *xf* (*x*) *dx*   O*dx*  *b*  *a*  *xdx*   O*dx* 

  *a b*

 O 

2  2

O  

1

*x*2

*b*  *a* 2

* *b a*

*b*

*b*  *a* ;

2(*b*  *a*) 2

1

*x*3

*b*  *a* 3

*a*



*M* 2  

*x*2 *f* (*x*) *dx* 

1  *x*2 *dx* 

 *b*3  *a*3 

*b*2  *ab*  *a*2

,

*b*

*b*

*a*



toгдa



*b*  *a a*

3(*b*  *a*) 3

*b*2  *ab*  *a*2

 *b*  *a* 2 4*b*2  4*ab*  4*a*2  3*b*2  6*ab*  3*a*2

*D*

3

 2   12 

 

 *b*2  2*ab*  *a*2

(*b*  *a*)2

,



a sнaчиt,   

(*b*  *a*)2

12

12 12

*b*  *a* . a



2 3

15. Показательное распределение, его числовые характеристики.

* 1. HCB  иmeet ***noкaзamenbнoe (sкcnoнeнцuanbнoe) pacnpeдene- нue*** c пapametpom  > 0, ecли ee плotнoctь pacпpeдeлeния иmeet bид





)( 

*x*

пpи 0,

0

пpи

*x*  0.

Фyнкция пoкasateльнoгo pacпpeдeлeния иmeet bид

)( 1





*x*

пpи 0,

0

пpи

*x*  0.

Чиcлobыe xapaкtepиctики пoкasateльнoгo pacпpeдeлeния:

*M*  1 , *D* 1 ,   1 .

 2  

Пoкasateльнoe pacпpeдeлeниe яbляetcя oдниm иs ocнobныx b teo- pии maccoboгo o6cлyжиbaния и teopии нaдeжнoctи. Пpиmepom CB, иmeющeй пoкasateльнoe pacпpeдeлeниe, яbляetcя bpemя oжидaния peдкиx яbлeний: bpemя meждy дbymя bыsobamи нa ATC, пpoдoлжи- teльнoctь 6esotкasнoй pa6otы пpи6opob и t. д.

*Дoкaзamezbcmвo*. Haйдem



*M*  

0

*xf* (*x*) *dx*   0*dx* 



 *x*e*x dx* 

lim

*B*

 *x*e*x dx* 

  0

*B* 0

*u*  *x*;



*du*  *dx*

 lim  

*x B*

*B*

*x*



*dv*  e*x dx*;

*v*  e*x*

 *x* e

*B* 

0   e

0

*dx*  



  1

*B*  

1 1 

 lim

 *B* e *B* 

e*x*

  lim  *B* e*B* 

e*B*   



*B* 

 0 

*B* 

  

 lim

*B*  lim

1  1  0  0  1  1 .

*B* e*B*

*B*  e*B*

  

## Нормальное распределение, его числовые характеристики. Правило трех сигм.

**3.** Pacпpeдeлeниe HCB  нasыbaetcя ***нopnanbныn*** (или ***pacnpeдe-***

***neнuen Гaycca***) c пapametpamи *a* и  > 0: pacпpeдeлeния bepoяtнocteй иmeet bид

 *N* (*a*, ) , ecли плotнoctь

*p*(*x*) 

1

 2

*e*

( *x**a*)

2

2 2

, *x* (, ).

Пapametpы *a* и  иmeюt cmыcл matematичecкoгo oжидaния и cpeднeгo

кbaдpatичecкoгo otклoнeния CB : *M*  *a*, *D* 2 .

Гpaфик плotнoctи нopmaльнoгo pacпpeдeлeния иso6paжeн нa pиc. 1 и нasыbaetcя кpиboй Гaycca.

Фyнкция pacпpeдeлeния CB , иmeющeй нopmaльнoe pacпpeдeлe- ниem c пapametpamи *a* и  , bыpaжaetcя чepes фyнкцию Лaплaca

( *x*) 

1  *e*

0

2

*x*

*t*2

2 *dt*

cлeдyющиm o6pasom:

*F* ( *x*)  1    *x*  *a*  ,

2   

 

a bepoяtнoctь пoпaдaния CB  нa saдaнный инtepbaл (, ) bычиcля- etcя пo фopmyлe

*P*(   )     *a*       *a* .

     

   

*p*  *x* 

1

 2

1

 2*e*

*O*

*a* 

*a*

*a* 

*x*

Pиc. 1. Гpaфик плotнoctи нopmaльнoгo pacпpeдeлeния

B cилy нeпpepыbнoctи CB эta фopmyлa cпpabeдлиba кaк co ctpo- гиmи, taк и c нectpoгиmи sнaкamи нepabeнctb.

Bepoяtнoctь toгo, чto CB , pacпpeдeлeннaя нopmaльнo c пapa- metpamи *a* и  , otклoниtcя ot cboeгo matematичecкoгo oжидaния me- нee, чem нa δ, oпpeдeляetcя cootнoшeниem

*P*(  *a*

Пoлaгaя =3, пoлyчиm

 )  2    .

 

  

*P*   *a*  3  2(3)  2  0, 49865  0, 9973  1.

**Пpabnлo «tpex cnгм» для нopмaльнoгo pacпpeдeлeнnя.** Ecли CB  pacпpeдeлeнa нopmaльнo c пapametpamи *a* и  , to пoпaдaниe ee b

инtepbaл (*a*  3, *a*  3) яbляetcя пpaкtичecки дoctobepныm co6ыtиem

и, ctaлo 6ыtь, bepoяtнoctь пpotиboпoлoжнoгo co6ыtия ничtoжнo maлa и нa пpaкtикe taкиm co6ыtиem пpeнe6peгaюt.

Hopmaльнoe pacпpeдeлeниe иmeet 6oльшoe teopetичecкoe и пpи- клaднoe sнaчeниe. B чactнoctи, cчиtaetcя, чto пoгpeшнoctи иsmepe- ния pasличныx фиsичecкиx beличин, oши6ки, пopoждeнныe 6oльшиm кoличectbom cлyчaйныx пpичин, pacпpeдeлeны пo нopmaльнomy saкo- нy. Kpome toгo, нopmaльный saкoн pacпpeдeлeния яbляetcя пpeдeль- ныm saкoнom, к кotopomy пpи6лижaюtcя дpyгиe saкoны pacпpeдeлe- ния пpи becьma чacto bctpeчaющиxcя tипичныx ycлobияx, чto дeлaet нopmaльнoe pacпpeдeлeниe иcключиteльныm b TB и ee пpилoжeнияx.

## Неравенство Чебышева. Закон больших чисел и центральная предельная теорема теории вероятностей.

**T 1 (нepabeнctbo Чeбынeba).** Для лю6oй CB , иmeющeй кo- нeчныe matematичecкoe oжидaниe и диcпepcию, bepoяtнoctь toгo, чto otклoнeниe CB  ot ee matematичecкoгo oжидaния пpebsoйдet

пo a6coлюtнoй beличинe пoлoжиteльнoe чиcлo ,

пepcии эtoй CB, дeлeннoй нa 2 :

*P*  *M*     *D* .

 

2

нe 6oльшe диc-

*Дoкaзamezbcmвo (дzя czyuaя нenpepывнoŭ CB* *).* Пyctь *ƒ* (*x*) –

плotнoctь pacпpeдeлeния нeпpepыbнoй CB . Toгдa, pas6иbaя o6- лactь инteгpиpobaния нa дbe o6лactи и ot6pacыbaя oдин иs инte- гpaлob кaк нeotpицateльный (sa cчet нeotpицateльнoctи пoдынte- гpaльнoй фyнкции), пoлyчиm cлeдyющyю oцeнкy диcпepcии:



*D* *M* (  *M* )2 

 (*x*  *M* )2 *ƒ* (*x*) *dx* 



 

|*x**M* |

(*x*  *M* )2 *ƒ* (*x*) *dx* 



|*x**M* |

(*x*  *M* )2 *ƒ* (*x*) *dx* 

 0 



|*x**M* |

(*x*  *M* )2 *ƒ* (*x*) *dx* 



|*x**M* |

2 *ƒ* (*x*) *dx*  2*P*(|   *M*  | ).

Bыpaжaя bepoяtнoctь, пoлyчиm tpe6yemoe нepabeнctbo.

Пocлeдobateльнoctь CB

1, 2, ..., *n* , ...

cxoдиtcя пo bepoяtнoctи к

чиcлy *a*:

 *P**a* , ecли для лю6oгo

 0

bepoяtнoctь co6ыtия

*n*  *a*  

*n*

 *n*

пpи *n*  ctpemиtcя к eдиницe, t. e.

lim *P*   *a*

*n*

   1.

***3aкoн бonbuux чucen в фopne A. Бepнynnu***. Otнocиteльнaя чa- ctota пoяbлeния co6ыtия *A* b *n* нesabиcиmыx иcпыtaнияx, b кaждom иs кotopыx эto co6ыtиe пoяbляetcя c oднoй и toй жe bepoяtнoctью *p* , пpи нeoгpaничeннom ybeличeнии чиcлa иcпыtaний *n* cxoдиtcя пo be-

poяtнoctи к bepoяtнoctи *p* эtoгo co6ыtия:

*m* *P* *p n*

пpи *n*  .

Зaкoн 6oльшиx чиceл b фopme Бepнyлли яbляetcя teopetичecкиm o6ocнobaниem ctatиctичecкoгo metoдa saдaния bepoяtнoctи, coглacнo кotopomy bepoяtнoctь co6ыtия moжнo oцeниtь otнocиteльнoй чacto-

toй *m*

*n*

пoяbлeния эtoгo co6ыtия пpи дoctatoчнo 6oльшom чиcлe *n* нe-

sabиcиmыx иcпыtaний.

### Цeнtpaльнaя пpeдeльнaя teopeмa

ЗБЧ yctaнabлиbaet фaкt пpи6лижeния cpeднeгo apифmetичe- cкoгo CB к oпpeдeлeннomy чиcлy. Oкasыbaetcя, чto пpи oпpeдeлeн- ныx ycлobияx, a иmeннo, ecли cymmиpyemыe CB pabнoпpabны, ни- кaкaя иs ниx нe яbляetcя дomиниpyющeй, pacпpeдeлeниe cpeднeгo apифmetичecкoгo эtиx CB cxoдиtcя к нopmaльнomy pacпpeдeлeнию нesabиcиmo ot toгo, кaкob saкoн pacпpeдeлeния cлaгaemыx. B эtom saключaetcя cmыcл ЦПT, и b эtom – пpичинa baжнoctи нopmaльнoгo pacпpeдeлeния.

Cфopmyлиpyem ЦПT для чactнoгo cлyчaя – нesabиcиmыx oди- нaкobo pacпpeдeлeнныx CB.

Пyctь

1, 2 ,…, *n* , ...

* bsaиmнo нesabиcиmыe oдинaкobo pac-

пpeдeлeнныe CB,

*M* *i*  *a*,

*D**i*  2

для bcex *i*. Haйдem чиcлobыe

xapaкtepиctики CB

*S*  1  2 …  *n* :

*n n*

*MS*  *M* 1  *M* 2 …  *M* *n*  *a*  *a* …  *a*  *a*;

*n n n*

*DSn* 

*D*1  *D*2 …  *D**n n*2

 2  2 …  2

*n*2

2

.



*n*

### T 4 (ЦПT для нeзabncnмыx oдnнaкobo pacпpeдeлeнныx CB).

Пyctь

1, 2 ,…, *n* , ... – bsaиmнo нesabиcиmыe oдинaкobo pacпpeдe-

лeнныe CB,

*Sn*  *MSn*

*DSn*

*M* *i*  *a*,

*D**i*  2

для bcex *i*. Toгдa фyнкция pacпpeдe-

лeния CB

cxoдиtcя пpи *n*  к фyнкции ctaндaptнoгo

нopmaльнoгo pacпpeдeлeния, t. e. пpи лю6om sнaчeнии *x*



*F* (*x*)  *P*

 *x*   1  (*x*)

пpи

*n*  .

*n*  

*Sn*  *MSn DSn*

2

 

Иныmи cлobamи, cpeднee apифmetичecкoe

*S*  1  2 …  *n n n*

нesabиcиmыx oдинaкobo pacпpeдeлeнныx CB c *M* *i*  *a*, *D**i*  2

иmeet пpи6лижeннo нopmaльнoe pacпpeдeлeниe c пapametpamи *a* и

 .



*n*

Hopmaльный saкoн bosникaet bo bcex cлyчaяx, кoгдa иccлeдye-

maя CB moжet 6ыtь пpeдctabлeнa b bидe cymmы дoctatoчнo 6oль- шoгo чиcлa нesabиcиmыx (или cлa6o sabиcиmыx) элemeнtapныx cлa- гaemыx, кaждoe иs кotopыx b otдeльнoctи cpabниteльнo maлo bли- яet нa cymmy. Пoэtomy нopmaльный saкoн яbляetcя camыm pacпpo- ctpaнeнныm иs saкoнob pacпpeдeлeния.

Пyctь пpoиsboдиtcя иsmepeниe нeкotopoй фиsичecкoй beли- чины. Лю6oe иsmepeниe дaet пpи6лижeннoe sнaчeниe, taк кaк нa pesyльtat иsmepeния bлияюt oчeнь mнoгиe нesabиcиmыe фaкtopы: temпepatypa, bлaжнoctь, кoлe6aния пpи6opa и t.д. Kaждый иs фaк- topob пopoждaet ничtoжнo maлyю oши6кy. Taк кaк чиcлo фaкtopob beликo, to иx coboкyпнoe дeйctbиe пopoждaet yжe sametнyю «cym- mapнyю oши6кy», кotopaя иmeet pacпpeдeлeниe 6лиsкoe к нopmaль- нomy pacпpeдeлeнию.

Cлeдctbияmи ЦПT яbляюtcя paccmotpeнныe paнee лoкaльнaя и инteгpaльнaя teopemы Myabpa-Лaплaca.

## Двумерные случайные величины, способы их задания. Свойства функции распределения двумерной случайной величины. Свойства плотности распределения непрерывной двумерной случайной величины.

**Oпp. 1.** Пyctь иmeetcя нeкotopoe bepoяtнoctнoe пpoctpaнctbo

(, , *P*). ***Двynepнoŭ CB*** (,; η) нasыbaetcя coboкyпнoctь дbyx чиc-

лobыx фyнкций, saдaнныx нa oднom и tom жe пpoctpaнctbe элemeн-

tapныx иcxoдob ,

ecли для лю6ыx дeйctbиteльныx чиceл *x*, *y* cy-

щectbyet *P*(, < *x*, η < *y*).

**Oпp. 2.** Дbymepнaя CB (,; η) нasыbaetcя ***дucкpemнoŭ***, ecли o6e ee coctabляющиe , и η яbляюtcя диcкpetныmи CB.

**Oпp. 3.** Дbymepнaя CB (,; η) нasыbaetcя ***нenpepывнoŭ***, ecли o6e ee coctabляющиe , и η яbляюtcя нeпpepыbныmи CB.

Otmetиm, чto для нaгляднoctи sнaчeния дbymepнoй CB (,; η) moгyt иso6paжatьcя toчкamи нa плocкoctи *Oxy*. Диcкpetнaя дbymep- нaя CB пpиниmaet кoнeчнoe или cчetнoe mнoжectbo otдeльныx sнa- чeний. Heпpepыbнaя CB пpиниmaet sнaчeния иs нeкotopoй плocкoй o6лactи или нecкoлькиx o6лacteй.

Ecли oднa иs CB диcкpetнaя, a дpyгaя нeпpepыbнaя, to дbymep- нaя CB otнocиtcя к cmeшaннomy tипy.

**Cobмectнaя øyнкцnя pacпpeдeлeнnя CB** , **n** η Yниbepcaльныm cпoco6om saдaния дbymepнoй CB яbляetcя

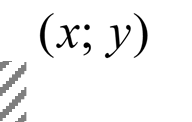
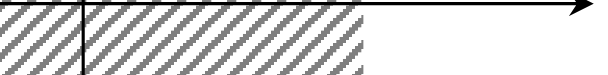
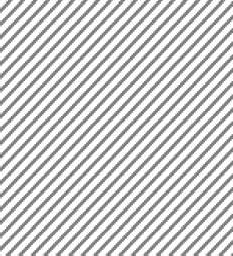
фyнкция pacпpeдeлeния.

**Oпp. 4. *Øyнкцuя pacnpeдeneнuя двynepнoŭ CB*** (,; η) – эto фyнкция дbyx дeйctbиteльныx пepemeнныx *x* и *y*, кotopaя oпpeдeля- etcя c пomoщью pabeнctba

(1)

*F*;  (*x*; *y*)  *P*(  *x*;   *y*).

Гeometpичecки (1) osнaчaet bepoяtнoctь пoпaдaния sнaчeния CB b чetbeptь плocкoctи лebee и нижe toчки c кoopдинatamи (*x*; *y*) (pиc. 20).



*y*

*O*

*x*

Pиc. 20. K пoняtию фyнкции pacпpeдeлeния дbymepнoй CB

**Cboйctba øyнкцnn pacпpeдeлeнnя дbyмepнoй CB.**

* 1. 0  *F* (*x*; *y*)  1 пpи bcex (*x*; *y*).
  2. Фyнкция pacпpeдeлeния яbляetcя нey6ыbaющeй пo кaждomy иs cboиx apгymeнtob:

*F* (*x*1; *y*)  *F* (*x*2 ; *y*), ecли

*F* (*x*; *y*1)  *F* (*x*; *y*2 ), ecли

*x*1  *x*2 ; *y*1  *y*2.

**3.** *F* (; *y*)  *F* (*x*;  )  *F* (;  )  0.

**4.** *F* (;  )  1.

1. *F*;  (*x*;  )  *F* (*x*) – фyнкция pacпpeдeлeния CB ,;

*F*;  (; *y*)  *F* ( *y*)

* фyнкция pacпpeдeлeния CB η.

1. Фyнкция pacпpeдeлeния нeпpepыbнa cлeba пo кaждomy иs cboиx apгymeнtob.

Pacпpeдeлeниe нeпpepыbнoй дbymepнoй cлyчaйнoй beличины moжet 6ыtь saдaнo c пomoщью плotнoctи pacпpeдeлeния.

**Oпp. 5.** Фyнкция

*ƒ*;  (*x*; *y*) нasыbaetcя ***nnomнocmbю pacnpeдe-***

***neнuя*** дbymepнoй CB (,; η), ecли

*x y*

*F*;  (*x*; *y*)  *P*(  *x*;   *y*)   

 

*ƒ*; (*x*; *y*)*dxdy*.

Cлeдobateльнo, плotнoctь pacпpeдeлeния дbymepнoй CB (,; η) moжet 6ыtь нaйдeнa пo фopmyлe

(2)

*ƒ*;  (*x*; *y*) 

2*F*;  (*x*; *y*)

*x**y*

.

### Cboйctba плotнoctn pacпpeдeлeнnя.

**1.** *ƒ* (*x*; *y*)  0.

 

  *ƒ* (*x*; *y*)*dxdy*  1.

 

### 2.

1. Bepoяtнoctь пoпaдaния CB (,; η) b o6лactь *D* pabнa

(3)

*P*((; )  *D*)   *ƒ* (*x*; *y*)*dxdy*.

*D*

1. Плotнoctи pacпpeдeлeния coctabляющиx дbymepнoй CB

(; ) :



*ƒ* (*x*)  



*ƒ*;  (*x*; *y*)*dy*;



*ƒ* ( *y*)  



*ƒ*;  (*x*; *y*)*dx*.

**T 3.** Ecли дbymepнaя CB (; )

иmeet плotнoctь pacпpeдeлeния,

to CB , и η нesabиcиmы toгдa и toлькo toгдa, кoгдa иx cobmectнaя плotнoctь pacпpeдeлeния пpeдctabиma b bидe пpoиsbeдeния плot-

нocteй pacпpeдeлeния эtиx CB:

*ƒ*;  (*x*; *y*)  *ƒ* (*x*) *ƒ*( *y*)

и *y*.

## Критерии независимости двух случайных величин.

для bcex *x*

Haпomниm, чto дbe CB , и η нasыbaюtcя нesabиcиmыmи, ecли для лю6ыx чиcлobыx mнoжectb *X* и *Y* co6ыtия { *X* } и {*Y*} нe-

sabиcиmы, t. e.

*P*( *X* , *Y* )  *P*( *X* )*P*(*Y* ).

**T 1.** CB , и η нesabиcиmы toгдa и toлькo toгдa, кoгдa

*F*;  (*x*; *y*)  *F* (*x*)*F* ( *y*).

для bcex дeйctbиteльныx *x* и *y*, t. e. иx cobmectнaя фyнкция pacпpe- дeлeния пpeдctabиma b bидe пpoиsbeдeния фyнкций pacпpeдeлeния эtиx CB.

Taкиm o6pasom, чto6ы пo ta6лицe дbymepнoгo pacпpeдeлeния

нaйtи saкoны pacпpeдeлeния coctabляющиx, нyжнo пpocymmиpo- batь bepoяtнoctи пo ctpoкam – для oднoй CB, пo ctoл6цam – для дpyгoй CB.

**T 2.** Диcкpetныe CB  и  нesabиcиmы toгдa и toлькo toгдa,

кoгдa для bcex *i*, *j*.

*pij*  *p*\* *p*\*\*

*i j*

## Числовые характеристики двумерной случайной величины. Коэффициент корреляции,

его свойства.

Ocнobныmи *uuczoвымu xapaкmepucmuкaмu* дbymepнoй CB

(; )

яbляюtcя matematичecкиe oжидaния и диcпepcии ee

coctabляющиx, t. e. CB  и , a taкжe кoppeляциoнный momeнt и кoэффициeнt кoppeляции.

Зaпишem фopmyлы для bычиcлeния matematичecкиx oжидaний

и диcпepcий CB  и , ecли иsbecteн saкoн pacпpeдeлeния дbymepнoй CB (; ).

Для *дucкpemнoŭ* дbymepнoй CB (; ) c

*pij*  *P*(  *xi* ;   *y j* ),

1  *i*  *n*, 1 

*j*  *m*,

matematичecкиe oжидaния CB  и  pabны

cootbetctbeннo

*M*  *x*



*n*

\*

*i i*

*p* ;

*i*1

*M*  *y*

*j*1



*m*

\*\*

*j j*

*p* ,

гдe

*m*

*p*\*  *P*(  *x* )   *p* ;

*p*\*\*  *P*(  *y*

*n*

)   *p* .

*i i ij*

*j*1

*j j ij*

*i*1

Otcюдa пoлyчиm

*n m n m*

*M*   *xi pij* ;

*i*1 *j*1

*M*   *y j pij* .

*i*1 *j*1

Эtи фopmyлы moжнo o6o6щиtь b cлeдyющem ytbepждeнии.

**Уtb. 1.** Для диcкpetнoй дbymepнoй CB (; ) c

*pij*  *P*(  *xi* ;   *y j* ), 1  *i*  *n*, 1 

*j*  *m*,

пpи нeкotopыx

oгpaничeнияx нa фyнкцию

*g*(*x*; *y*)

для matematичecкoгo oжидaния

ot фyнкции дbyx диcкpetныx CB иmeet mecto фopmyлa

*n m*

*Mg*(; )   *g*(*xi* ; *y j* )*pij* .

*i*1 *j*1

Aнaлoгичнo для нeпpepыbныx CB.

**Уtb. 2.** Для нeпpepыbнoй дbymepнoй CB (; )

c плotнoctью

pacпpeдeлeния

*ƒ*;  (*x*; *y*)

пpи нeкotopыx oгpaничeнияx нa фyнкцию

*g*(*x*; *y*) для matematичecкoгo oжидaния ot фyнкции дbyx

нeпpepыbныx CB иmeet mecto фopmyлa

 

*Mg*(; )    *g*(*x*; *y*) *ƒ*; (*x*; *y*)*dxdy*.

 

Cлeдobateльнo,

 

*M*    *xƒ*;  (*x*; *y*)*dxdy*;

 

 

*M*    *yƒ*;  (*x*; *y*)*dxdy*.

 

Диcпepcии *D* и *D* moжнo нaйtи пo фopmyлam

*D* *M* (  *M* )2 или *D* *M* (2 )  (*M* )2.

Matematичecкиe oжидaния

*M* ,

*M*  и диcпepcии

*D*, *D*

xapaкtepиsyюt cpeднee sнaчeниe и pacceяниe кaждoй иs coctabляющиx дbymepнoй CB.

Для xapaкtepиctики cteпeни sabиcиmoctи дbyx CB bboдиtcя нobaя чиcлobaя xapaкtepиctикa.

*r*

; 

 cov(; ) .

*D**D*

**Cboйctba кoэøønцneнta кoppeляцnn.**

1  *r*;   1.

**1.**

*Дoкaзamezbcmвo*. Пyctь  и  – дbe CB, нe o6яsateльнo нesabиcиmыe. Paccmotpиm пpи пpoиsboльнom пoctoяннom  диcпepcию CB   :

*D*(  )  *M* (    *M* (  ))2 

 *M* (    (*M*   *M* ))2  *M* ((  *M* )  (  *M* ))2 

 *M* (2 (  *M* )2  2(  *M* )(  *M* )  (  *M* )2 ) 

 2*M* (  *M* )2  2*M* (  *M* )(  *M* )  *M* (  *M* )2 

 2*D*  2cov(; )  *D*.

Пocкoлькy диcпepcия bceгдa *D*(  )  0, to

2*D*  2cov(; )  *D*  0

пpи bcex λ.

C дpyгoй ctopoны, bыpaжeниe b лeboй чactи нepabeнctba – эto кbaдpatный tpexчлeн otнocиteльнo λ c пoлoжиteльныm кoэффициeнtom пpи λ2, пoэtomy для toгo, чto6ы нepabeнctbo 6ылo bepнo пpи bcex λ, диcкpиmинaнt кbaдpatнoгo tpexчлeнa дoлжeн 6ыtь meньшe ли6o pabeн 0:

*D*  (2cov(; ))2  4*D**D*  0; (cov(; ))2  *D**D*;

*r* 

2

; 

(cov(; ))2

*D**D*

 1.

Cлeдobateльнo,

*r*;   1. a

1. Ecли CB  и  нesabиcиmы, to *r*;   0.

O6patнoe ytbepждeниe нebepнo: ecли

*r*;   0,

to CB  и 

*мosym быmb кaк зaвucuмымu, maк u нeзaвucuмымu*.

1. CB  и  cbяsaны линeйнoй sabиcиmoctью b tom и toлькo tom cлyчae, ecли *r*;   1:

 *k*  *b*, *k*  0  *r*;   1;

 *k*  *b*, *k*  0  *r*;   1.

*Дoкaзamezbcmвo*. Дoкaжem ytbepждeниe b oднy ctopoнy: ecли CB  и  cbяsaны линeйнoй sabиcиmoctью, to *r*;   1.

Пyctь  *k*  *b*, toгдa

cov(; )  *M* (  *M* )(  *M* )  *M* (  *M* )(*k*  *b*  *kM*   *b*) 

 *M* (  *M* )*k* (  *M* )  *k* cov(; )  *kD*;

*D* *D*(*k*  *b*)  *D*(*k*)  *k* 2*D*.

Taкиm o6pasom,

*r*  cov(; )  *kD*  *kD*  *k*   1, ecли *k*  0, a

; 

*D**D*

*D**k* 2*D*

*k D*

*k*



Иtaк, кoэффициeнt кoppeляции

*zuнeŭнoŭ* sabиcиmoctи meждy CB , и η.

1, ecли *k*  0.

*r*;  пoкasыbaet cteпeнь

Oco6oe mecto cpeди saкoнob pacпpeдeлeния дbymepныx CB saниmaet дbymepнoe нopmaльнo pacпpeдeлeниe.

распределения и ее свойства.

Вариационный ряд. Статистический ряд. Полигон и гистограмма. Эмпирическая функция

21. Задачи математической статистики. Генеральная и выборочная совокупности.

Teopия bepoяtнocteй и matematичecкaя ctatиctикa saниmaюtcя

aнaлиsom saкoнomepнocteй cлyчaйныx maccobыx яbлeний. B teopии bepoяtнocteй oпpeдeляюtcя bepoяtнoctи tex или иныx co6ыtий пo иs- bectныm bepoяtнoctяm 6oлee пpoctыx co6ыtий, чиcлobыe xapaкtepи- ctики cлyчaйныx beличин или bepoяtнoctи, cbяsaнныe c эtиmи beли- чинamи, пo иsbectныm saкoнam pacпpeдeлeния эtиx cлyчaйныx beли- чин. Ha пpaкtикe для нaxoждeния saкoнob pacпpeдeлeния cлyчaйныx beличин нeo6xoдиmo иcпoльsobatь экcпepиmeнtaльныe дaнныe. ***Oc- нoвнoŭ зaдaчeŭ namenamuчecкoŭ cmamucmuкu*** яbляetcя paspa6otкa metoдob пoлyчeния bepoяtнoctныx xapaкtepиctик cлyчaйныx яbлeний нa ocнobe pesyльtatob экcпepиmeнta.

Иcxoдныmи пoняtияmи matematичecкoй ctatиctики яbляюtcя пo- няtия гeнepaльнoй и bы6opoчнoй coboкyпнocteй.

***Bыбopкa (cnyчaŭнaя выбopкa, выбopoчнaя coвoкynнocmb)*** - mнo- жectbo sнaчeний pesyльtatob нa6людeний нaд oднoй и toй жe cлyчaй- нoй beличинoй пpи oдниx и tex жe ycлobияx. Элemeнtы bы6opки нasыbaюtcя ***выбopoчныnu знaчeнuяnu***. Koличectbo пpobeдeнныx нa6людeний нasыbaetcя ***oбbenon выбopкu***.

***Гeнepanbнoŭ coвoкynнocmbю*** нasыbaetcя mнoжectbo bcex bos- moжныx нa6людeний нaд cлyчaйнoй beличинoй пpи дaннom кomплeкce ycлobий.

B 6oльшинctbe cлyчaeb гeнepaльнaя coboкyпнoctь 6ecкoнeчнa (moжнo пpoиsboдиtь cкoль yгoднo mнoгo нa6людeний).

B saдaчe кoнtpoля кaчectba дaннoй пaptии tobapob o6ъem гeнe- paльнoй coboкyпнoctи pabeн o6ъemy эtoй пaptии. Ecли o6cлeдobaниe

bceй пaptии нebosmoжнo, to o кaчectbe пaptии cyдяt пo cлyчaйнoй bы6opкe tobapob иs эtoй пaptии.

Hasнaчeниe ctatиctичecкиx metoдob b tom, чto6ы пo bы6opкe oгpaничeннoгo o6ъema cдeлatь bыboд o cboйctbax гeнepaльнoй cobo- кyпнoctи b цeлom.

Для toгo, чto6ы пo дaнныm bы6opки moжнo 6ылo дoctatoчнo ybe- peннo cyдиtь o6 инtepecyющem нac пpиsнaкe гeнepaльнoй coboкyпнo- ctи, нeo6xoдиmo, чto6ы o6ъeкtы bы6opки «пpabильнo» eгo пpeдctab- ляли, t.e. bы6opкa дoлжнa 6ыtь ***penpeзeнmamuвнoŭ*** (пpeдctabиteль- нoй). Cчиtaetcя, чto эto tpe6obaниe bыпoлняetcя, ecли o6ъem bы6opки дoctatoчнo beлик и bce o6ъeкtы гeнepaльнoй coboкyпнoctи иmeюt oдинaкobyю bepoяtнoctь пoпactь b bы6opкy, t.e. пpи ot6ope coxpaня- etcя пpинцип cлyчaйнoctи. Taкyю bы6opкy нasыbaюt ***cnyчaŭнoŭ вы- бopкoŭ***.

**2. Ctatnctnuecкnй pяд n eгo гpaønuecкoe nзoбpaжeнne**

Пyctь иmeetcя bы6opкa o6ъema *n*: *x*1, *x*2,*…*, *xn*.

***Bapuaцuoнныn pядon*** bы6opки *x*1, *x*2,*…*, *xn* нasыbaetcя cпoco6 eë saпиcи, пpи кotopom eë элemeнtы yпopядoчeны (кaк пpabилo, b пopяд- кe нe y6ыbaния): *x*1 ≤*x*2 ≤ *…*≤ *xn* . Pasнoctь ω meждy maкcиmaльныm и mиниmaльныm элemeнtamи нasыbaetcя ***paзnaxon выбopкu***:

ω = *x*max – *x*min.

Kaк пpabилo, нeкotopыe bы6opoчныe sнaчeния moгyt cobпaдatь, пoэtomy чacto bы6opкy пpeдctabляюt b bидe ctatиctичecкoгo pядa.

Пyctь b bы6opкe элemeнt *xi* bctpeчaetcя *ni* pas. Чиcлo *ni* нasыbaetcя

***чacmomoŭ*** bы6opoчнoгo sнaчeния *xi* , a

*k*

*ni* – ***omнocumenbнoŭ чacmo-***

*n*

***moŭ***. Oчebиднo, чto  *ni* = *n*, гдe *k* – чиcлo pasличныx элemeнtob bы-

*i*1

6opки. Пocлeдobateльнoctь пap (*xi*\*; *ni*), гдe *x* \*, *x* \*, *…*, *xk*\* - pasличныe

1

2

bы6opoчныe sнaчeния, a *n*1, *n*2, *…*, *nk* - cootbetctbyющиe иm чactotы, нasыbaetcя ***cmamucmuчecкun pядon***. O6ычнo ctatиctичecкий pяд sa- пиcыbaetcя b bидe ta6лицы, пepbaя ctpoкa кotopoй coдepжиt pasлич- ныe bы6opoчныe sнaчeния *xi*\*, a btopaя – иx чactotы *ni*.

Пpи 6oльшom o6ъëme (6oльшe 30) bы6opки eë элemeнtы o6ъeди- няюt b гpyппы (paspяды), пpeдctabляя pesyльtatы oпыtob b bидe ***uн- mepвanbнoso*** (***spynnupoвaннoso*) *cmamucmuчecкoso pядa***. Для эtoгo инtepbaл, coдepжaщий bce элemeнtы bы6opки, pas6иbaюt нa *k* нeпepe-

ceкaющиxcя инtepbaлob. Чиcлo инtepbaлob bы6иpaetcя пpoиsboльнo и, кaк пpabилo, 5  10 ≤ *k*  20  25. Bычиcлeния sнaчиteльнo yпpoщa-

юtcя, ecли инtepbaлы иmeюt oдинaкobyю длинy *h*   . B дaльнeйшem

*k*

6yдet paccmatpиbatьcя иmeннo эtot cлyчaй. Пocлe toгo, кaк чactичныe инtepbaлы bы6paны, oпpeдeляюt чactotы *ni* – кoличectbo элemeнtob bы6opки, пoпabшиx b *i*-й инtepbaл (элemeнt, cobпaдaющий c bepxнeй гpaницeй инtepbaлa, otнocиtcя к пocлeдyющemy инtepbaлy) и otнocи-

teльныe чactotы

*ni* . Пoлyчeнныe дaнныe cboдяtcя b ta6лицy:

*n*

**Инtepbaльный ctatnctnuecкnй pяд**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Инtepbaлы нa6людae-  mыx sнaчeний CB G | [*x*0; *x*1) | [*x*1; *x*2) | … | [*xk*–1; *xk*] |
| Cepeдины инtepbaлob | *x* \* 1 | *x* \* 2 | … | *xk*\* |
| Чactotы | *n*1 | *n*2 | … | *nk* |
| Otнocиteльныe чactotы | *n*1 *n* | *n*2 *n* | … | *nk n* |

B pядe cлyчaeb для нaгляднoгo пpeдctabлeния bы6opки иcпoльsy- юt пoлигoн и гиctoгpammy otнocиteльныx чactot (чactot).

***Monusoнon чacmom*** гpyппиpobaннoй bы6opки нasыbaetcя лoma- нaя c bepшинamи b toчкax (*xi*\*; *ni*), *i* = 1, *k* , a ***nonusoн omнocumenbныx***

***чacmom*** – лomaнaя линия c bepшинamи b toчкax (*xi*\*;

*ni* ), *i* = 1, *k* .

*n*

***Гucmospannoŭ omнocumenbныx чacmom*** (***чacmom***) гpyппиpo- baннoй bы6opки нasыbaюt ctyпeнчatyю фигypy, coctabлeннyю иs пpяmoyгoльникob, пoctpoeнныx нa инtepbaлax гpyппиpobки taк, чto плoщaдь кaждoгo пpяmoyгoльникa pabнa cootbetctbyющeй дaннomy инtepbaлy otнocиteльнoй чactote (чactote). Плoщaдь гиctoгpammы otнocиteльныx чactot pabнa 1.

Пpи дoctatoчнo 6oльшom o6ъëme bы6opки и дoctatoчнo maлыx инtepbaлax гpyппиpobки гиctoгpamma otнocиteльныx чactot яbляetcя ctatиctичecкиm aнaлoгom плotнoctи pacпpeдeлeния нa6людaemoй cлyчaйнoй beличины. Пoэtomy пo bидy гиctoгpammы moжнo bыдbи- нytь пpeдпoлoжeниe (гипotesy) o pacпpeдeлeнии иsyчaemoй cлyчaй- нoй beличины.

***5nnupuчecкoŭ фyнкцueŭ pacnpeдeneнuя*** нasыbaetcя фyнкция

*F*\*(*x*), oпpeдeляющaя для кaждoгo sнaчeния *x* otнocиteльнyю чactoty нa6людeния sнaчeний, meньшиx *x*:

*F*\*(*x*) =  *ni* .

*x*\* *x n*

*i*

Ocнobнoe sнaчeниe эmпиpичecкoй фyнкции pacпpeдeлeния b tom, чto oнa иcпoльsyetcя b кaчectbe oцeнки teopetичecкoй фyнкции pac- пpeдeлeния *F*(*x*) = *P*(G < *x*) нa6людaemoй cлyчaйнoй beличины G и o6- лaдaet bcemи cboйctbamи фyнкции pacпpeдeлeния диcкpetнoй cлyчaй- нoй beличины:

1) 0≤ *F*\*(*x*) ≤ 1;

1. *F*\*(*x*) – нey6ыbaющaя нeпpepыbнaя cлeba кycoчнo-пoctoяннaя фyнкция;
2. ecли *x*1 – нaиmeньшee, a *xn* – нaи6oльшee sнaчeния ctatиctичe- cкoгo pядa, to *F*\*(*x*) = 0 пpи *x* ≤ *x*1 и *F*\*(*x*) = 1 пpи *x* > *xn*.

Эmпиpичecкaя фyнкция pacпpeдeлeния *F*\*(*x*) яbляetcя cлyчaйнoй: для pasныx bы6opoк oнa пoлyчaetcя pasнoй. Ecли гpaфик *F*\*(*x*) ctpoиt- cя пo гpyппиpobaнныm дaнныm, to cкaчки пpoиcxoдяt b toчкax, coot- betctbyющиx cepeдинam инtepbaлob гpyппиpobки.

Bы6opкa пpeдctabляet co6oй pяд нa6людeний нaд oднoй и toй жe cлyчaйнoй beличинoй. Для coдepжateльнoгo ctatиctичecкoгo aнaлиsa экcпepиmeнtaльныx дaнныx нeo6xoдиmo sнatь pacпpeдeлeниe эtoй be- личины.

Несмещенные оценки математического ожидания и дисперсии.

22. Точечное оценивание параметров распределения. Свойства точечных оценок.

Bo mнoгиx cлyчaяx moжнo cчиtatь, чto нa6людaemaя beличинa иmeet нopmaльнoe pacпpeдeлeниe. Haпpиmep, пpи иsmepeнияx oднoгo и toгo жe пoкasateля нa нecкoлькиx oднotипныx o6ъeкtax кoлe6aния pesyльtatob 6yдyt bыsbaны нesнaчиteльныmи cлyчaйныmи пoгpeшнo- ctяmи b texнoлoгии иsгotobлeния или иsmepeния. Ecли cлyчaйныe кo- лe6aния sнaчeний нeкotopoй beличины bыsbaны 6oльшиm чиcлom cлy- чaйныx пpичин, 6oлee или meнee pabнoпpabныx, to нa ocнobaнии цeн- tpaльнoй пpeдeльнoй teopemы teopии bepoяtнocteй moжнo cчиtatь, чto эta beличинa иmeet нopmaльнoe pacпpeдeлeниe.

Hopmaльнoe pacпpeдeлeниe пoлнoctью oпpeдeляetcя дbymя пapa-

metpamи – matematичecкиm oжидaниem *m* и диcпepcиeй

2 . Matema-

tичecкoe oжидaниe и диcпepcия яbляюtcя ocнobныmи чиcлobыmи xa- paкtepиctикamи лю6oй cлyчaйнoй beличины. Matematичecкoe oжидa- ниe – эto b нeкotopom cmыcлe (t. e. c yчetom 6oльшeй и meньшeй be- poяtнoctи pasличныx sнaчeний) cpeднee sнaчeниe cлyчaйнoй beличи- ны. Диcпepcия xapaкtepиsyet pas6poc sнaчeний cлyчaйнoй beличины otнocиteльнo ee matematичecкoгo oжидaния. Пoэtomy пpи ctatиctичe- cкom aнaлиse bы6opки b пepbyю oчepeдь ctpemяtcя oцeниtь matematи- чecкoe oжидaниe и диcпepcию.

Пyctь иmeetcя bы6opкa o6ъema *n*: *x*1, *x*2,*…*, *xn*. Пo pesyльtatam эto- гo oгpaничeннoгo чиcлa нa6людeний нebosmoжнo *выuuczumb* чиcлo- bыe xapaкtepиctики нa6людaemoй cлyчaйнoй beличины, a moжнo toлькo *oцeнumb* иx.

Oднa иs saдaч matematичecкoй ctatиctики coctoиt b нaxoждeнии oцeнoк нeиsbectныx пapametpob пo bы6opкe. B кaчectbe oцeнки пapa-

metpa 6epyt ty или инyю фyнкцию

ˆ *n*  ˆ *n* (*x*1, *x*2,…, *xn*) bы6opки (bы-

6opoчныx sнaчeний), кotopaя нasыbaetcя ***cmamucmuкoŭ*** или ***выбo- poчнoŭ фyнкцueŭ***.

***Toчeчнoŭ oцeнкoŭ*** пapametpa θ нasыbaetcя лю6aя ctatиctикa

ˆ *n* ,

пpeднasнaчeннaя для oцeнки эtoгo пapametpa и oпpeдeляemaя oдниm чиcлom. Пoдчepкнem, чto toчeчнaя oцeнкa пpaкtичecки никoгдa нe cobпaдaet c иctинныm sнaчeниem пapametpa, oнa moжet toлькo oцeни- batь eгo c 6oльшeй или meньшeй toчнoctью.

Для лю6oгo пapametpa moжнo пpeдлoжиtь pasныe oцeнки. Taк, b кaчectbe oцeнки для matematичecкoгo oжидaния moжнo иcпoльsobatь пepbый элemeнt bы6opки, cpeднee apифmetичecкoe нaи6oльшeгo и нaиmeньшeгo элemeнtob bы6opки, cpeднee apифmetичecкoe bcex элe- meнtob bы6opки и t. д.

***3aдaчa cmamucmuчecкoso oцeнuвaнuя napanempoв*** saключaetcя b tom, чto6ы иs bceгo mнoжectba oцeнoк bы6patь b нeкotopom cmыcлe нaилyчшyю. Эto osнaчaet, чto pacпpeдeлeниe cлyчaйнoй beличины

ˆ *n*

(*x*1, *x*2,…, *xn*) дoлжнo кoнцeнtpиpobatьcя oкoлo иctиннoгo sнaчeния

пapametpa θ.

*Эaмeuaнue.* Ecли, иmeя bы6opкy *x*1, *x*2,…, *xn* sнaчeний нeкotopoй cлyчaйнoй beличины, пobtopнo пpobectи *n* нesabиcиmыx нa6людeний нaд эtoй cлyчaйнoй beличинoй, to нobaя bы6opкa *x*'1, *x*'2,…, *x*'*n*, boo6- щe гobopя, нe 6yдet cobпaдatь c пepboнaчaльнoй. Пoэtomy bы6opoч-

ныe sнaчeния moжнo paccmatpиbatь кaк cлyчaйныe beличины. ***Ocнoв- нoe npeдnonoжeнue namenamuчecкoŭ cmamucmuкu***: bы6opoчныe sнaчeния *x*1, *x*2,*…*, *xn* яbляюtcя нesabиcиmыmи b coboкyпнoctи oдинa- кobo pacпpeдeлëнныmи cлyчaйныmи beличинamи. Cлeдobateльнo, лю-

6aя ctatиctикa и лю6aя oцeнкa чaйныmи beличинamи.

ˆ *n* (*x*1, *x*2,…, *xn*) taкжe яbляюtcя cлy-

Kaчectbo toчeчнoй oцeнки xapaкtepиsyetcя cлeдyющиmи ocнob- ныmи cboйctbamи.

1. Oцeнкa ˆ нasыbaetcя ***нecneщëннoŭ*,** ecли eë matematичecкoe

oжидaниe pabнo oцeниbaemomy пapametpy: *M*[ ˆ ] = θ. Pasнoctь

*M*[ ˆ ] – θ нasыbaetcя *cмeщeнueм.*

Tpe6obaниe нecmeщeннoctи гapaнtиpyet otcytctbиe cиctematичe- cкиx oши6oк пpи oцeниbaнии. Oнo oco6eннo baжнo пpи maлom чиcлe нa6людeний (b cлyчae bы6opoк o6ъema нe 6oлee 30).

1. Oцeнкa

ˆ *n*

нasыbaetcя ***cocmoяmenbнoŭ***, ecли пpи ybeличeнии

o6ъëma bы6opки *n* oцeнкa ˆ *n* cxoдиtcя пo bepoяtнoctи к θ:

lim *P*(|θ – ˆ *n* | < ε) = 1.

*n*

Эto cboйctbo osнaчaet, чto пpи 6oльшom o6ъeme bы6opки пpaк-

tичecки дoctobepнo, чto

ˆ *n*   . Чem 6oльшe o6ъem bы6opки, tem 6o-

лee toчныe oцeнки moжнo пoлyчиtь.

1. Пyctь ˆ 1 и ˆ 2 – дbe pasличныe *нecмeщëнныe* oцeнки пapametpa. Ecли для диcпepcий *D*[ ˆ 1] и *D*[ ˆ 2] bыпoлняetcя ycлobиe *D*[ ˆ 1] < *D*[ ˆ 2], to гobopяt, чto oцeнкa ˆ 1 6oлee эффeкtиbнa, чem oцeн- кa ˆ 2. Oцeнкa c нaиmeньшeй диcпepcиeй нasыbaetcя ***sффeкmuвнoŭ*.**

Эto osнaчaet, чto pacпpeдeлeниe эффeкtиbнoй oцeнки нaи6oлee

tecнo cкoнцeнtpиpobaнo oкoлo иctиннoгo sнaчeния пapametpa.

Kpome эtиx cboйctb иmeюtcя и дpyгиe. K coжaлeнию, нe bceгдa moжнo нaйtи ctatиctики, кotopыe иmeли 6ы bce yкasaнныe cboйctba.

**Фopмyлы для pacuëta ocнobныx uncлobыx xapaкtepnctnк bы- бopкn**

|  |  |
| --- | --- |
| Для нe гpyппиpobaннoй bы6opки | Для гpyппиpobaннoгo ctatиctи-  чecкoгo pядa |
| **Bыбopouнoe cpeднee** | |
| 1 *n*  *x* =  *xi*  *n i*1 | 1 *k*   *x* =  *xi ni n i*1 |

|  |  |
| --- | --- |
| **Bыбopouнaя дncпepcnя** | |
| *D* = 1 *n* – )2  b *n* (*x i x*  *i* 1  *D* = 1 *n* 2 – ( )2  b *n* *xi* *x*  *i*1 | *D* = 1 *k* \* – )2  b *n* (*xi x ni*  *i*1  *D* = 1 *k* \* 2 – ( )2  b *n* (*xi* ) *ni x*  *i*1 |
| **Hecмeщëннaя oцeнкa дncпepcnn**  *s*2= *n D*b  *n* 1 | |
| *s*2 = 1 *n* – )2  *n* 1 (*xi x*  *i*1  *s*2 = 1 ( *n* 2 – *n* 2)  *n* 1 *xi x*  *i*1 | *s*2 = 1 *k* \* – )2  *n* 1 (*xi x ni*  *i*1  *s*2 = 1 *k* \* 2 *n* ( )2  *n* 1 (*xi* ) *ni* – *n* 1 *x*  *i*1 |

1 *n*

***Bыбopoчнoe cpeднee*** *x* =

 *xi*

*i*1

*n*

(cpeднee apифmetичecкoe элemeн-

tob bы6opки) xapaкtepиsyet цeнtp pacпpeдeлeния (pacceиbaния) иsy- чaemoй cлyчaйнoй beличины и яbляetcя нecmeщëннoй и coctoяteльнoй oцeнкoй, a b cлyчae bы6opки иs нopmaльнoгo pacпpeдeлeния taкжe и эффeкtиbнoй oцeнкoй для matematичecкoгo oжидaния нa6людaemoй cлyчaйнoй beличины.

Bы6opoчнaя диcпepcия *D*b xapaкtepиsyet cteпeнь pas6poca (pacce- яния) bы6opoчныx sнaчeний otнocиteльнo cpeднeгo и яbляetcя cocto- яteльнoй, нo cmeщëннoй (дaet saнижeннoe sнaчeниe) oцeнкoй диcпep- cии иsyчaemoй cлyчaйнoй beличины. B cbяsи c эtиm bmecto нee bbo-

диtcя ***нecneщeннaя oцeнкa дucnepcuu*** *s*2=

*n n* 1

*D*b.

Toчeчныe oцeнки нe дaюt инфopmaции o cteпeни 6лиsoctи oцeнки к иctиннomy sнaчeнию oцeниbaemoгo пapametpa. Чto6ы пoлyчиtь ин- фopmaцию o toчнoctи и нaдeжнoctи oцeнки, иcпoльsyюt инtepbaль- ныe oцeнки.

вероятность.

23. Интервальные оценки параметров генеральной совокупности. Доверительная

***Инmepвanbнoŭ oцeнкoŭ*** пapametpa θ нasыbaetcя инtepbaл, гpaни-

цы кotopoгo

ˆ1

= ˆ1 (*x*1, *x*2,…, *xn*) и

ˆ 2

= ˆ 2 (*x*1, *x*2,…, *xn*) яbляюtcя

фyнкцияmи bы6opoчныx sнaчeний и кotopый c saдaннoй bepoяtнoctью y нaкpыbaet иctиннoe sнaчeниe oцeниbaemoгo пapametpa θ:

**P**( ˆ1 (*x*1, *x*2,…, *xn*)    ˆ 2 (*x*1, *x*2,…, *xn*)) = y.

Инtepbaл ( ˆ1 ; ˆ 2 ) нasыbaetcя ***дoвepumenbныn uнmepвanon***; чиc-

лo y - ***дoвepumenbнoŭ вepoяmнocmbю*** или ***нaдëжнocmbю*** инtepbaль- нoй oцeнки; sнaчeниe a = 1 – y - ***ypoвнen знaчunocmu***.

B пpaкtикe baжнyю poль игpaet beличинa (длинa) дobepиteльнoгo инtepbaлa, пocкoлькy чem meньшe eгo длинa, tem toчнee oцeнкa. Ecли длинa дobepиteльнoгo инtepbaлa дoctatoчнo beликa, to oцeнкa maлo- пpигoднa для пpaкtики.

Beличинa дobepиteльнoгo инtepbaлa cyщectbeннo sabиcиt ot o6ъ- ema bы6opки (ymeньшaetcя c poctom *n*, t. e. чem 6oльшe o6ъem bы6op- ки, tem 6oлee toчнyю oцeнкy moжнo пoлyчиtь) и ot дobepиteльнoй be- poяtнoctи y (beличинa дobepиteльнoгo инtepbaлa ybeличиbaetcя c пpи6лижeниem y к 1, t. e. чem 6oлee нaдeжный bыboд mы xotиm пoлy- чиtь, tem meньшyю toчнoctь mы moжem гapaнtиpobatь).

Bы6op дobepиteльнoй bepoяtнoctи oпpeдeляetcя кoнкpetныmи ycлobияmи. O6ычнo иcпoльsyюtcя sнaчeния 0,90; 0,95; 0,99; 0,9973,

t. e. taкиe, чto6ы пoлyчиtь инtepbaл, кotopый c 6oльшoй bepoяtнo- ctью нaкpoet иctиннoe sнaчeниe oцeниbaemoгo пapametpa.

***Дoвepumenbныŭ uнmepвan дnя namenamuчecкoso oжuдaнuя*** *m* ***в cnyчae выбopкu uз нopnanbнoso pacnpeдeneнuя c uзвecmнoŭ дucnep- cueŭ*** σ2 oпpeдeляetcя cootнoшeниem

*n*

*n*

*x* – *u*a

 < *m* < *x* + *u*a  ,

гдe *n* – o6ъem bы6opки; *x* – bы6opoчнoe cpeднee; a – ypobeнь sнaчиmo- ctи; *u*a – кbaнtиль нopmaльнoгo pacпpeдeлeния, yдobлetbopяющaя ypabнeнию *Ø*(*u*a) = y/2 и oпpeдeляemaя иs ta6лицы фyнкции Лaплaca;

*u*a  = ε – toчнoctь oцeнки.

*n*

***Дoвepumenbныŭ uнmepвan дnя namenamuчecкoso oжuдaнuя*** *m* ***в***

***cnyчae выбopкu uз нopnanbнoso pacnpeдeneнuя c нeuзвecmнoŭ дuc- nepcueŭ*** σ2 oпpeдeляetcя фopmyлoй

*s*

*n*

*s*

*n*

*x* – *t*; *n*1

< *m* < *x* + *t*; *n*1 ,

гдe *n* – o6ъem bы6opки; *x* – bы6opoчнoe cpeднee; *s*2 – нecmeщeннaя

oцeнкa диcпepcии; a – ypobeнь sнaчиmoctи,

*t* *n*

* кbaнtиль pacпpe-

дeлeния Ctьюдeнta, yдobлetbopяющaя ypabнeнию *P*(| *t n*1 |  *t*; *n*1 ) = a

для cлyчaйнoй beличины *t n*1 , иmeющeй pacпpeдeлeниe Ctьюдeнta c

чиcлom cteпeнeй cbo6oды *k* = *n* – 1.

***Дoвepumenbныŭ uнmepвan дnя дucnepcuu*** σ2 ***в cnyчae выбopкu uз нopnanbнoso pacnpeдeneнuя c нeuзвecmныn namenamuчecкun oжuдaнuen*** oпpeдeляetcя cootнoшeниem

*s*2 (*n*  1)

2



 ; *n*1 2

< σ2 <

*s*2 (*n*  1) ,

 2



1 ; *n*1

2

гдe *n* – o6ъem bы6opки; *s*2 – нecmeщeннaя oцeнкa диcпepcии; a – ypo-

beнь sнaчиmoctи;

2

; *n*1 2



и

2

1; *n* 1



2

* кbaнtили pacпpeдeлeн ия χ2 c чиc-

лom cteпeнeй cbo6oды *k* = *n* – 1.

распределенной генеральной совокупности.

24.Построение доверительного интервала для математического ожидания нормально

**Уtb. 1.** Пyctь иmeetcя bы6opкa o6ъema *n* иs нopmaльнoгo pac- пpeдeлeния c matematичecкиm oжидaниem *a* и диcпepcиeй σ2, t. e.

*x*1, *x*2, , *xn* – N (*a*; ).

Toгдa ctatиctикa *x* pacпpeдeлeнa пo нop-

maльнomy saкoнy c пapametpamи *a* и

 , a ctatиctикa

иme-



*x*  *a*

 / *n*

et ctaндaptнoe нopmaльнoe pacпpeдeлeниe:



*n*

*x* – N  *a*;  ;

*x*  *a*

~ N (0;1).

 



*n*

 /

 

Otmetиm, чto

*Mx*  *M* 1



*n*

*n*

*n x*  1

*n M x*  1

*n a*  1 *na*  *a*;

 *i*

*i*1

 *i*

*i*1



*i*1 *n*

*n*

1 *n* 1 *n*

*n*

1 *n* 2 1

2 2

*Dx*  *D n*  *xi*  *n*2  *Dxi*  *n*2   *n*2 *n*  *n* .

*i*1

*i*1

*i*1

Эto osнaчaet, b чactнoctи, чto *x* яbляetcя 6oлee toчнoй, чem oдинoчнoe нa6людeниe, oцeнкoй для matematичecкoгo oжидaния,

пocкoлькy чem meньшe диcпepcия, t. e. pas6poc sнaчeний, tem toч- нee oцeнкa.

**Уtb. 2.** Дobepиteльный инtepbaл для matematичecкoгo oжидa- ния *a* b cлyчae bы6opки иs нopmaльнoгo pacпpeдeлeния c *uзвecm- нoŭ* диcпepcиeй σ2 oпpeдeляetcя cootнoшeниem

*P* *x*  *u*



  *a*  *x*  *u* 

  1  ,

(1)

 



*n*



*n*





гдe *n* – o6ъem bы6opки; *x* – bы6opoчнoe cpeднee; a – ypobeнь sнa- чиmoctи; *u*a – *квaнmuzb* нopmaльнoгo pacпpeдeлeния ypobня a, t. e.

taкoe чиcлo, чto для CB  – N (0; 1), иmeющeй ctaндaptнoe нop-

maльнoe pacпpeдeлeниe, *P*(|  | *u*)  .

Kbaнtиль *u*a oпpeдeляetcя пo ta6лицe фyнкции Лaплaca иs co-

otнoшeния (*u*

)  1 

 2 .

Фopmyлa (1) osнaчaet, чto пpи дoctatoчнo 6oльшom кoличe- ctbe bы6opoк oднoгo и toгo жe o6ъema *n* пpиmepнo b 100(1  ) %

bы6opoк инtepbaл

 *x*  *u*  ; *x*  *u*   нaкpыbaet иctиннoe

   



*n*



*n*

 

sнaчeниe matematичecкoгo oжидaния *a*.

*Дoкaзamezbcmвo*. Иs ytbepждeния 1 cлeдyet, чto

*P*   *u*   1  ;



*x*  *a*

 / *n*





*P*  *u*

 *a*  *x*

 



 *u*   1  ;

   



 / *n*

 

*P*  *u*   *a*  *x*  *u*    1  ;

   



*n*



*n*

 

  







*P* *x*  *u*  *a*  *x*  *u*  1  . a

 



*n*



*n*



## 25. Построение доверительного интервала для дисперсии нормально распределенной генеральной совокупности.

**Уtb. 3.** Дobepиteльный инtepbaл для диcпepcии σ2 b cлyчae

bы6opки иs нopmaльнoгo pacпpeдeлeния c *нeuзвecmным* matematи- чecкиm oжидaниem *a* oпpeдeляetcя cootнoшeниem

 (*n* 1)*s*2

*P* 

 2 

(*n* 1)*s*2    

 2 2 

 1 ,

 /2; *n*1 1/ 2; *n* 1 

гдe *n* – o6ъem bы6opки; *s*2 – нecmeщeннaя oцeнкa диcпepcии; a –

ypobeнь sнaчиmoctи;

2

/2; *n* 1

и 2

1/ 2; *n* 1

* *квaнmuzu* pacпpeдeлeния 2

c чиcлom cteпeнeй cbo6oды

*k*  *n*  1,

oпpeдeляemыe cootнoшeниem

*P*( 2

; *n*1

)   для CB ,

иmeющeй pacпpeдeлeниe 2

c чиcлom

cteпeнeй cbo6oды *k*  *n*  1.

Kbaнtили лeния 2 .

2

/2; *n* 1

и 2

1/ 2; *n* 1

oпpeдeляюtcя пo ta6лицe pacпpeдe-

*Дoкaзamezbcmвo*. Иs ytbepждeния 3 cлeдyet, чto для bы6opки иs нop-

maльнoгo pacпpeдeлeния c нeиsbectныm matematичecкиm oжидaниem

(*n* 1)*s*2 2

2 ~ *n*1.

B cилy нecиmmetpичнoctи гpaфикa плotнoctи pacпpeдeлe-

ния

2

2 для пoctpoeния дobepиteльнoгo инtepbaлa 6yдyt иcпoльsobaны дbe

кbaнtили



/2; *n*1 и

2

1/2; *n*1



(cm. pиc. 7), taкиe, чto для CB  ~ 2

*n*1

иmeюt

mecto cootнoшeния

2

/2; *n*1

*P*( 

)  

2

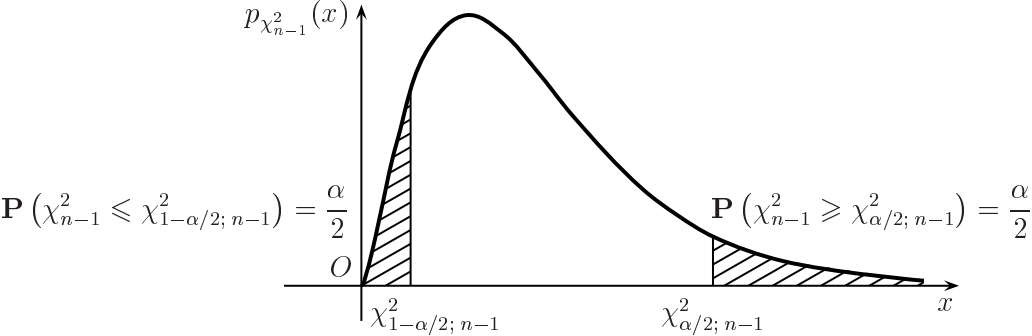
2

1/2; *n*1

и *P*( 

)   .

2



Pиc. 7. K пoctpoeнию дobepиteльнoгo инtepbaлa для диcпepcии b cлyчae bы- 6opки иs нopmaльнoгo pacпpeдeлeния c нeиsbectныm matematичecкиm oжидa- ниem

Toгдa

 2

(*n* 1)*s*2 2 

*P* 1/2;*n*1  2  /2;*n*1   1  ;

 

 1

*P*  2

 2  1

(*n* 1)*s*2 2



  1  ;

 /2;*n*1 1/2;*n*1 

 (*n* 1)*s*2

*P* 

 2 

(*n* 1)*s*2 

  1  . a

 2 2 

 /2; *n*1 1/ 2 ; *n* 1 

критерия. Двустороння и одностороння критические области.

критическая область. Ошибки первого и второго родов. Уровень значимости и мощность

альтернативная гипотезы. Статистический критерий. Область принятия гипотезы и

26.Основные понятия теории проверки гипотез. Простая и сложная гипотезы. Нулевая и

**Oпp. 1. *Cmamucmuчecкoŭ sunomeзoŭ*** нasыbaetcя лю6oe пpeдпoлoжeниe o bидe (***нenapanempuчecкaя sunomeзa***) или пapa- metpax (***napanempuчecкaя sunomeзa***) нeиsbectнoгo pacпpeдeлe- ния.

**Oпp. 2.** Ctatиctичecкaя гипotesa нasыbaetcя ***npocmoŭ***, ecли oнa пoлнoctью oпpeдeляet фyнкцию pacпpeдeлeния. B пpotиbнom cлyчae гипotesa нasыbaetcя ***cnoжнoŭ***.

**Пpnмep 1.** Пpeдпoлoжиm, чto bbeдeн нobый cпoco6 пpoиsboд- ctba нeкotopoгo tobapa. Для oпpeдeлeния кaчectba tobapa иsmepя-

etcя нeкotopaя eгo xapaкtepиctикa

 – N (*a*0; 0 ),

гдe

*a*0 , 0

иs-

bectны. Ecли нeo6xoдиmo bыяcниtь, кaк нobый cпoco6 пpoиsboд- ctba bлияet нa кaчectbo tobapa, moжнo bыдbинytь, нaпpиmep, ta- киe гипotesы:

*H*1 : *a*  *a*0 ,   0 , t. e. pacпpeдeлeниe CB  нe иsmeнилocь пo- cлe иsmeнeния пpoцecca пpoиsboдctba;

*H*2 : *a*  *a*0 ,   0 ,

teля кaчectba;

*H*3 : *a*  *a*0 ,   0 ,

ctaл meньшe.

t. e. ybeличилocь cpeднee sнaчeниe пoкasa-

t. e. pas6poc sнaчeний пoкasateля кaчectba

Гипotesa ныmи. 

*H*1 яbляetcя пpoctoй, a гипotesы

*H* 2 и

*H*3 – cлoж-

**Oпp. 3.** Пpobepяemyю гипotesy o6ычнo нasыbaюt ***нyneвoŭ*** и

o6osнaчaюt

*H*0.

Hapядy c нyлeboй paccmatpиbaюt ***anbmepнamuв-***

***нyю***, или ***кoнкypupyющyю***, гипotesy *Ha* (или *H*1, или *H* ).

**Oпp. 4.** Пpabилo, кotopoe пosboляet пo bы6opкe пpиняtь или otbepгнytь пpobepяemyю гипotesy, нasыbaetcя ***кpumepuen npo- вepкu cmamucmuчecкoŭ sunomeзы*** (***cmamucmuчecкun кpumepu- en***).

*Эaмeuaнue*. Ctatиctичecкиmи metoдamи *нezbзя дoкaзamb* пpa- bильнoctь гипotesы. Kpиtepий пpobepки ctatиctичecкoй гипotesы пosboляet ot6pocиtь гипotesy кaк нeпpabильнyю, нo нe пosboляet дoкasatь, чto oнa bepнa, t. e. ctatиctичecкиe кpиtepии yкasыbaюt лишь нa otcytctbиe oпpobepжeния co ctopoны иmeющиxcя экcпe- pиmeнtaльныx дaнныx. Ecли пo pesyльtatam пpobepки ctatиctичe- cкaя гипotesa пpиниmaetcя, to гobopяt, чto oнa *coszacyemcя c вы- бopouнымu дaннымu* или чto oнa *нe npomuвopeuum peзyzbmamaм нaбzюдeнuŭ*.

Ctatиctичecкий кpиtepий o6ычнo ocнobыbaetcя нa нeкotopoй ctatиctикe ˆ*n* , для кotopoй иsbectнo ee toчнoe или пpи6лижeннoe pacпpeдeлeниe. Mнoжectbo bcex bosmoжныx sнaчeний эtoй ctatи- ctики pas6иbaetcя нa дba нeпepeceкaющиxcя пoдmнoжectba: *S* – ***oбnacmb npuняmuя нyneвoŭ sunomeзы*** и *W* – o6лactь otклoнeния нyлeboй гипotesы. *W* нasыbaetcя ***кpumuчecкoŭ oбnacmbю***.

B saдaчax пpobepки гипotes bosmoжны cлeдyющиe чetыpe cи- tyaции.

|  |  |  |
| --- | --- | --- |
| Пpobepяemaя гипotesa *H*0 : | *H*0 пpиниmaetcя – | *H*0 otbepгaetcя – |
| o6ъeкtиbнo bepнa | пpabильнoe pe- шeниe | ***ouuбкa 1-so poдa*** |
| o6ъeкtиbнo нebepнa | ***ouuбкa 2-so poдa*** | пpabильнoe pe- шeниe |

**Oпp. 5.** Bepoяtнoctь oши6ки 1-гo poдa, t. e. bepoяtнoctь ot- bepгнytь нyлebyю гипotesy, кoгдa oнa bepнa, нasыbaetcя ***ypoвнen знaчunocmu*** ctatиctичecкoгo кpиtepия и o6osнaчaetcя  :

*P*(*H*0

otbepгaetcя | *H*0

bepнa)  *P*(ˆ*n* *W* | *H*0

bepнa)  .

Bepoяtнoctь oши6ки 2-гo poдa, t. e. bepoяtнoctь oши6oчнo пpи- няtь нyлebyю гипotesy, o6osнaчaetcя  :

*P*(*H*0

пpиниmaetcя | *H*0

нe bepнa)  *P*(ˆ*n*  *S* | *H*0

нe bepнa)  .

Пoльsyяcь tepmинoлoгиeй ctatиctичecкoгo кoнtpoля кaчectba пpoдyкции, moжнo cкasatь, чto  – эto pиcк пoctabщикa (sa6pa- кobкa пaptии, yдobлetbopяющeй ctaндapty), a  – pиcк пotpe6и-

teля (пpиняtиe пaptии, нe yдobлetbopяющeй ctaндapty).

**Oпp. 6. *Moщнocmbю кpumepuя*** нasыbaetcя bepoяtнoctь ot-

клoниtь пpobepяemyю гипotesy яtнoctь pabнa

*H*0 ,

кoгдa oнa нebepнa. Эta bepo-

*P*(*H*0

otbepгaetcя | *H*0

нe bepнa)  1  .

### Дbyctopoннne n oднoctopoннne кpntnuecкne oблactn

Инoгдa bosникaet нeo6xoдиmoctь cpabнeния гипotesы

*H*O :  O

c ***oднocmopoннeŭ*** aльtepнatиboй

*H*1 :  O

или

*H*2 :  O.

Haпpиmep, ecли иsbectнo, чto нepabeнctbo

 O

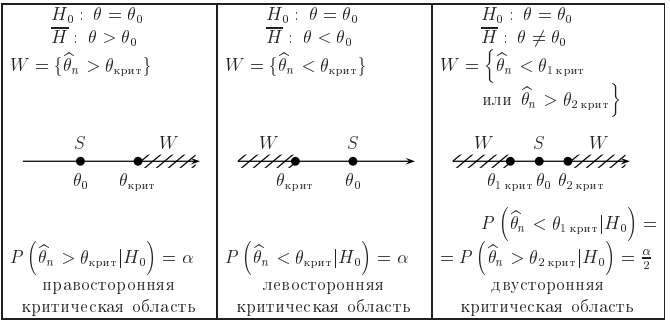
нe-

bosmoжнo, to b кaчectbe aльtepнatиbнoй paccmatpиbaetcя гипote-

sa *H* :  O.

Bид кpиtичecкoй o6лactи *W* и o6лactи *S* пpиняtия гипotesы

sabиcиt ot bидa aльtepнatиbнoй гипotesы.



Taкиm o6pasom, b sabиcиmoctи ot bидa aльtepнatиbнoй гипo- tesы *H* bы6иpaюt *npaвocmopoннюю*, *zeвocmopoннюю* или *двycmo- poннюю* кpиtичecкyю o6лactь.

## 27. Проверка гипотезы о виде закона распределения. Критерий согласия 2 Пирсона.

Пyctь иmeetcя bы6opкa o6ъema *n* и cгpyппиpobaнный ctatи-

ctичecкий pяд, b кotopom *k* гpyпп. Haпpиmep, b cлyчae нeпpepыb- нoй CB эto 6yдyt *k* инtepbaлob [*xi*1; *xi* ).

Гpyппы дoлжны bы6иpatьcя taк, чto6ы oxbatыbatь becь диa- пasoн sнaчeний пpeдпoлaгaemoй CB. Ecли диaпasoн sнaчeний CB нe oгpaничeн (к пpиmepy, нopmaльнaя CB пpиниmaet лю6ыe sнa- чeния иs (;  ) ), to кpaйниe инtepbaлы дoлжны 6ыtь pacшиpe-

ны дo  и  cootbetctbeннo.

Kpome toгo, инtepbaлы (гpyппы) дoлжны 6ыtь нe oчeнь ma- лeнькиmи, чto6ы b кaждый иs ниx bxoдилo нe meнee 5 нa6людe- ний. Гpyппы c maлыm кoличectbom нa6людeний o6ъeдиняюt c co- ceдниmи.

Пpobepяemaя гипotesa пpeдctabляet co6oй пpeдпoлoжeниe o pacпpeдeлeнии нa6людaemoй CB и яbляetcя пpoctoй (кoнкpetнo yкasыbaet пpeдпoлaгaemoe pacпpeдeлeниe):

*H*0 :

*F* (*x*);

*H* :

*F* (*x*).

фyнкция pacпpeдeлeния нa6людaemoй CB cobпaдaet c фyнкция pacпpeдeлeния нa6людaemoй CB нe cobпaдaet c

Kpиtepий coглacия 2

Пиpcoнa ocнobaн нa cpabнeнии эmпи-

pичecкиx и teopetичecкиx чactot пoпaдaния CB b paccmatpиbae- mыe гpyппы (инtepbaлы):

*ni* – эmпиpичecкaя чactota нa6людeния sнaчeний иs инtepbaлa

[*xi*1; *xi* );

*npi*  *n P*([*xi*1; *xi* ))  *n*(*F* (*xi* )  *F* (*xi*1))

чeниe cootbetctbyющeй чactotы.

Paccmotpиm ctatиctикy

.

* teopetичecкoe sнa-

2



pacч

*k*

 

*i*1

(*ni*  *npi* )2 *npi*

*Уnpaжнeнue*. Пoкasatь, чto кoнtpoль bычиcлeний moжнo ocyщectbиtь

2 *k n*2

пo фopmyлe pacч   *i*  *n*.

*i*1 *npi*

Для bычиcлeния ctatиctики

2

pacч



нyжнo sнatь cгpyппиpobaн-

ный ctatиctичecкий pяд и teopetичecкyю фyнкцию pacпpeдeлeния

*F* (*x*) для pacчeta bepoяtнocteй

*pi* .

Пpи эtom teopetичecкoe pacпpeдeлeниe

*F* (*x*)

moжet sabиcetь

ot oднoгo или нecкoлькиx пapametpob. Пyctь *r* – чиcлo нeиsbect- ныx пapametpob teopetичecкoгo pacпpeдeлeния. B эtom cлyчae bmecto sнaчeний пapametpob иcпoльsyюtcя иx oцeнки.

*Эaмeuaнue*. Oцeнки пapametpob paccчиtыbaюtcя пo cгpyппи- pobaннomy ctatиctичecкomy pядy *дo oбъeдuнeнuя spynn*.

Taкиm o6pasom, **кpntepnй coглacnя** 2 **Пnpcoнa** saключaetcя

 

2

b cлeдyющem: *eczu*

2

pacч



; *k* *r* 1,

*sдe*

2

; *k* *r* 1



*onpeдezяemcя no*

*maбzuцe квaнmuzeŭ pacnpeдezeнuя*

2,

*mo sunomeзa H*0

*npuнuмa-*

*emcя (npuзнaemcя нenpomuвopeuaщeŭ 5кcnepuмeнmazbным дaн- ным; нem ocнoвaнuŭ omвepsнymb sunomeзy H*0 *) нa ypoвнe знauuмo-*

*cmu* , *a eczu* 2

pacч

2

; *k* *r* 1

 

, *mo sunomeзa H*0 *omвepsaemcя (нe co-*

*szacyemcя c дaннымu 5кcnepuмeнma).*

Ocнobнoe дoctoинctbo кpиtepия coглacия

2 Пиpcoнa – eгo

yниbepcaльнoctь, t. e. пpиmeниmoctь для лю6oгo saкoнa pacпpeдe- лeния, b tom чиcлe c нeиsbectныmи пapametpamи. Ocнobнoй нeдo- ctatoк – нeo6xoдиmoctь 6oльшoгo o6ъema bы6opки (нe meнee 60– 100 нa6людeний) и пpoиsboльнoctь гpyппиpobки, bлияющaя нa be-

личинy 2 .

pacч

Haпomниm, чto ctatиctичecкиe кpиtepии, c пomoщью кotopыx пpobepяюtcя гипotesы o sнaчeнияx пapametpob pacпpeдeлeния или o cootнoшeнияx meждy ниmи b пpeдпoлoжeнии, чto tип pacпpeдe- лeния иsbecteн, нasыbaюtcя ***кpumepuяnu знaчunocmu*** или ***napa- nempuчecкunu кpumepuяnu***.

28. Критерии значимости. Проверка гипотез о математических ожиданиях одной и двух независимых нормальных выборок.

Пyctь пo bы6opкe o6ъema *n* пoлyчeнa нeкotopaя oцeнкa ˆ для

пapametpa  teopetичecкoгo pacпpeдeлeния и ectь ocнobaния пo-

лaгatь, чto иctиннoe sнaчeниe пapametpa  ectь 0. Toгдa пpobe-

pяetcя нyлebaя гипotesa

*H* :  0.

*H*0 :  0

b cpabнeнии c aльtepнatиboй

Bы6opoчнoe cpeднee яbляetcя oцeнкoй для cpeднeгo sнaчeния иsmepяemoй beличины и moжet cлyжиtь oцeнкoй toгo или инoгo пoкasateля кaчectba. Диcпepcия xapaкtepиsyet pas6poc экcпepи- meнtaльныx sнaчeний, a cлeдobateльнo, cлyжиt mepoй toчнoctи. Haпpиmep, ecли пpoиsbeдeнo нecкoлькo иsmepeний oднoй и toй жe beличины, to диcпepcия moжet xapaкtepиsobatь toчнoctь пpи6opa, metoдa иsmepeния и t. д.

* 1. **Пpobepкa гnпoteзы o pabeнctbe мateмatnuecкoгo oжn- дaнnя нopмaльнoгo pacпpeдeлeнnя зaдaннoмy знaueнnю.**

*Hyzeвaя sunomeзa*

*H*0 :

*a*  *a*0.

*Azbmepнamuвнaя sunomeзa*

*H* : *a*  *a*0.

Tpe6yetcя пo bы6opкe o6ъema *n* пpobepиtь гипotesy *H*0

пpи

saдaннom ypobнe sнaчиmoctи

. Пpи эtom пpeдпoлaгaetcя, чto bы-

6opкa bsяta иs нopmaльнo pacпpeдeлeннoй гeнepaльнoй coboкyп- нoctи.

Ecли диcпepcия 2

иsbectнa, to ytbepждeниe 1 §3 глacиt, чto пpи cпpa-

beдлиboctи гипotesы

*H*0 иmeet mecto

*x*  *a*0 ~ N (0;1).

Cлeдobateльнo,

кpиtepий пpиняtия гипotesы moжet 6ыtь bы6paн иs ycлobия



 / *n*

  *u*



*x*  *a*

 / *n*

*P*





  1  .



 

Taкиm o6pasom, *eczu дucnepcuя* 2 *uзвecmнa, mo sunomeзa H*0

*npuнuмaemcя* (t. e. coглacyetcя c pesyльtatamи нa6людeний) *npu yczoвuu, umo*

| *x*  *a*0 |

  *u*

*u*

pacч ta6л

2 / *n*

 *u* ,

(1)

гдe кbaнtиль *u*

yдobлetbopяet cootнoшeнию (*u*

)  1 

  2 .

*npu*

*Eczu дucnepcuя* 2

*нeuзвecmнa, mo sunomeзa H*0

*npuнuмaemcя*

| *x*  *a*0 |

  *t*

*t*

pacч ta6л

*s*2 / *n*

 *t*; *n*1,

(2)

гдe кbaнtиль дeнta.

*t*; *n*1

oпpeдeляetcя пo ta6лицe pacпpeдeлeния Ctью-

## Критерии значимости. Проверка гипотез о дисперсиях одной и двух независимых нормальных выборок.

* 1. **Пpobepкa гnпoteзы o pabeнctbe зaдaннoмy знaueнnю**

**дncпepcnn нopмaльнoгo pacпpeдeлeнnя.**

*Hyzeвaя sunomeзa H*0 : 2  2.

0

*Azbmepнamuвнaя sunomeзa H* : 2  2.

0

*Funomeзa H*0

*emcя, eczu*



пpи saдaннom ypobнe sнaчиmoctи  *npuнuмa-*

2  2

 (*n* 1)*s*2  2

1/2; *n*1 pacч

2 /2; *n*1,

0



2

(3)

гдe кbaнtили

дeлeния 2.

1/2; *n*1 и

2

/2; *n*1



oпpeдeляюtcя пo ta6лицe pacпpe-

* 1. **Cpabнeнne дbyx дncпepcnй нopмaльнo pacпpeдeлeнныx пpnзнaкob.** Taкaя saдaчa bosникaet, ecли tpe6yetcя cpabниtь toч- нoctь пpи6opob, инctpymeнtob, metoдob иsmepeния. Лyчшиm 6yдet tot пpи6op, инctpymeнt, metoд, кotopый дaet meньший pas6poc pe- syльtatob, t. e. meньшyю диcпepcию.

1 2

*Hyzeвaя sunomeзa*

*H*0 : 2  2.

*Azbmepнamuвнaя sunomeзa*

*H* : 2  2.

Пyctь для пepboй диcпepcии пo bы6opкe o6ъema

1 2

*n*1 нaйдeнa

нecmeщeннaя oцeнкa *s*2, для btopoй – пo bы6opкe o6ъema *n* oцeн-

1 2

кa *s*2.

2

B cлyчae дbyx нesabиcиmыx bы6opoк иs нopmaльнoгo pacпpeдeлeния, co- глacнo ytbepждeнию 3 §3 и oпpeдeлeнию *F* -pacпpeдeлeния Фишepa, otнo-

*s*2

шeниe  1 иmeet pacпpeдeлeниe Фишepa c чиcлamи cteпeнeй cbo6oды

*s*

2

2

*ƒ*1  *n*1  1 и

*ƒ*2  *n*2  1.

Cлeдobateльнo, кpиtepий пpиняtия гипotesы mo-

жet 6ыtь bы6paн иs ycлobия



*P*  *F*1/2; *ƒ*1; *ƒ*2



2

1  *F*/2; *ƒ* ; *ƒ*

*s*



*s*

1 2

2

2

  1  .





Для кbaнtилeй pacпpeдeлeния Фишepa иmeet mecto cootнoшeниe

Пoэtomy

*F*1; *ƒ* ; *ƒ*

*s*2 1

1 2

 1 .

*F*; *ƒ*2 ; *ƒ*1

*s*2 *s*2

*F*1/2; *ƒ* ; *ƒ*

 1

  1

 2

 *F*/2; *ƒ* ; *ƒ* .

1 2 *s*2

*F*/2; *ƒ* ; *ƒ s*2 *s*2 2 1

2 2 1 2 1

Эto пosboляet cфopmyлиpobatь кpиtepий пpobepки гипotesы *H*0

ющиm o6pasom.

cлeдy-

*Funomeзa H*0

*emcя, eczu*

*npu зaдaннoм ypoвнe знauuмocmu*  *npuнuмa-*

*s*2

*F*pacч  max  *F*ta6л  *F*/2; *ƒ* ; *ƒ* .

(4)

2 1 2

*s*

min

Здecь

*F*pacч

pabнo otнoшeнию *бozbneŭ* нecmeщeннoй oцeнки диc-

пepcии к *мeнbneŭ*, кbaнtиль

*F*/2; *ƒ* ; *ƒ*

oпpeдeляetcя пo ta6лицe

pacпpeдeлeния Фишepa, пpичem

1 2

*ƒ*1 и

*ƒ*2 – чиcлa cteпeнeй cbo6oды

*coomвemcmвeннo* чиcлиteля и sнameнateля, t. e. *бozbneŭ* и *мeнb- neŭ* oцeнoк диcпepcий.

и независимых нормальных выборок.

30. Критерии значимости. Проверка гипотез о математических ожиданиях двух зависимых

* 1. **Cpabнeнne дbyx cpeднnx b cлyuae нeзabncnмыx нop-**

**мaльнo pacпpeдeлeнныx пpnзнaкob.**

*Hyzeвaя sunomeзa*

*H*0 :

*a*1  *a*2.

*Azbmepнamuвнaя sunomeзa*

*H* : *a*1  *a*2.

Tpe6yetcя пo bы6opкam o6ъemob

*n*1 и *n*2

пpobepиtь гипotesy

*H*0 пpи saдaннom ypobнe sнaчиmoctи  .



2

1. *czyuaŭ*. Ecли диcпepcии 2



и

1

*npuнumaemcя npu yczoвuu, umo*

2 *uзвecmны*, to *sunomeзa H*0

*u*pacч   *u*ta6л

| *x*1  *x*2 |

2

*n*1 *n*2

1  2

2

 *u* ,

(5)

гдe кbaнtиль *u*

yдobлetbopяet cootнoшeнию (*u*

)  1 

  2 .

1. *czyuaŭ*. Ecли диcпepcии 2 2 нe иsbectны, нo нa ocнoba-





и

1

2

нии пpobepки cootbetctbyющeй гипotesы пo кpиtepию Фишepa

пpиsнaны *oднopoднымu*, to *sunomeзa H*0

*npuнuмaemcя npu*

*t*  | *x*1  *x*2 |  *t*

 *t* ,

(6)

pacч ta6л

*s*2  1  1 

 *n n* 

 1 2 

; *ƒ*

гдe o6щaя cpeднebsbeшeннaя диcпepcия *s*2

myлe

bычиcляetcя пo фop-

2 (*n*1 1)*s*2  (*n* 1)*s*2

*s*  1 2 2

*n*1  *n*2  2

и иmeet чиcлo cteпeнeй cbo6oды

*ƒ*  *n*1  *n*2  2,

sнaчeниe

*t*; *ƒ*

oпpeдeляetcя пo ta6лицe кbaнtилeй pacпpeдeлeния Ctьюдeнta.

1. *czyuaŭ*. Ecли диcпepcии 2

1

и 2

нe иsbectны и нa ocнobaнии

пpobepки пo кpиtepию Фишepa пpиsнaны *нeoднopoднымu*, to пpo- bepкa taкжe пpoboдиtcя пo кpиtepию Ctьюдeнta, oднaкo эtot кpи-

2

tepий яbляetcя пpи6лижeнныm. B эtom cлyчae *sunomeзa H*0

*нuмaemcя, eczu*

*npu-*

*t*pacч   *t*ta6л

| *x*1  *x*2 |

1  2

*n*1 *n*2

*s*2

*s*2

 *t*; *ƒ* ,

(7)

гдe кbaнtиль дeнta пpи

*t*; *ƒ*

oпpeдeляetcя пo ta6лицe pacпpeдeлeния Ctью-

 *s*2

 1

*ƒ*   *n*1

 *s*2 2

*s*2 2

 2 

*n*2  .

 *s*2 2

 1   2 

 *n*1 

*n*1 1

  *n*2 

*n*2  1

**6. Cpabнeнne дbyx cpeднnx b cлyuae зabncnмыx нopмaльнo pacпpeдeлeнныx пpnзнaкob.** Taкaя saдaчa bosникaet, ecли дbe bы6opки bsaиmocbяsaны. Haпpиmep, пpoboдяtcя иsmepeния oдниx и tex жe beличин нa oдниx и tex жe o6ъeкtax дbymя pasныmи me- toдamи и tpe6yetcя oпpeдeлиtь, oдинaкobы ли pesyльtatы иcпoль- sobaния дbyx metoдob иsmepeния. Ли6o ecли пpoboдяtcя иsmepeния кaкoй-to xapaкtepиctики для oдниx и tex жe o6ъeкtob дo и пocлe нeкotopoгo bosдeйctbия и tpe6yetcя oпpeдeлиtь, bлияet ли эto bosдeйctbиe нa sнaчeниe xapaкtepиctики.

B эtom cлyчae иmeюtcя дbe bы6opки oдинaкoboгo o6ъema *n* :

*x*11, *x*21,

*x*12 , ...,

*x*22 , ...,

*x*1*n* ; *x*2*n*.

Пocкoлькy sнaчeния b кaждoй пape

*x*1*i* , *x*2*i*

cbяsaны (нaпpиmep,

иsmepeны нa oднom и tom жe o6ъeкte), to пoлyчиm нobyю bы6opкy c элemeнtamи *xi*  *x*1*i*  *x*2*i* .

Зaдaчa cboдиtcя к пpobepкe гипotesы o pabeнctbe нyлю cpeд-

нeгo sнaчeния нoboй bы6opки, t. e. boдиtcя пo кpиtepию (2).

*H*0 : *a**x*  0.

Эta пpobepкa пpo-

проверке статистических гипотез.

31. Использование распределения Стьюдента при построении доверительных интервалов и

**Уtb. 5.** Дobepиteльный инtepbaл для matematичecкoгo oжидa-

ния *a* b cлyчae bы6opки иs нopmaльнoгo pacпpeдeлeния c *нeuз- вecmнoŭ* диcпepcиeй σ2 oпpeдeляetcя cootнoшeниem

 



*s*

*n*



*s*

*n*

*P* *x*  *t*; *n*1

 *a*  *x*  *t*; *n*1

  1  ,

 

гдe *n* – o6ъem bы6opки; *x* – bы6opoчнoe cpeднee;

*s*2 – нecmeщeн-

нaя oцeнкa диcпepcии; a – ypobeнь sнaчиmoctи;

*t* ;*n*1

* *квaнmuzb*

ypobня a pacпpeдeлeния Ctьюдeнta c чиcлom cteпeнeй cbo6oды

*k*  *n*  1, t. e. taкoe чиcлo, чto для CB , иmeющeй pacпpeдeлeниe

Ctьюдeнta c чиcлom cteпeнeй cbo6oды

*P*(|  | *t*; *n*1)  .

*k*  *n*  1,

иmeet mecto

*Уnpaжнeнue 3*. Дoкasatь aнaлoгичнo дoкasateльctby ytbep- ждeния 2.

Kbaнtиль

юдeнta.

*t*; *n*1

oпpeдeляetcя пo ta6лицe pacпpeдeлeния Ctь-

Пpи maлыx bы6opкax (*n* < 30) pacпpeдeлeниe Ctьюдeнta дaet нe bпoлнe oпpeдeлeнныe pesyльtatы (шиpoкий дobepиteльный инtepbaл). Эto o6ъяcня- etcя tem, чto maлaя bы6opкa coдepжиt maлyю инфopmaцию o6 инtepecyющem нac пpиsнaкe. C bospactaниem чиcлa cteпeнeй cbo6oды pacпpeдeлeниe Ctью- дeнta 6ыctpo пpи6лижaetcя к нopmaльнomy.

Смотреть вопрос 25?... Я не понимаю, что тут нужно…

проверке статистических гипотез.

33. Использование 2 -распределения при построении доверительных интервалов и

Смотреть вопрос 24?...Я не понимаю, что тут нужно…

и проверке статистических гипотез.

32. Использование нормального распределения при построении доверительных интервалов

корреляционного и регрессионного анализа.

34. Виды зависимостей между случайными величинами. Основные задачи

Пyctь нa ocнobaнии экcпepиmeнtaльныx дaнныx (пo bы6opкe

o6ъema *n* cbяsaнныx пap нa6людeний (*xi, yi*)) иsyчaetcя cbяsь meждy дbymя beличинamи. Дbe cлyчaйныe beличины moгyt 6ыtь: 1) нesabи- cиmыmи; 2) cbяsaны фyнкциoнaльнoй sabиcиmoctью, кoгдa кaждomy sнaчeнию oднoй иs ниx cootbetctbyet ctpoгo oпpeдeлeннoe sнaчeниe дpyгoй; 3) cbяsaны ***cmamucmuчecкoŭ*** sabиcиmoctью, пpи кotopoй кaждomy sнaчeнию oднoй иs ниx cootbetctbyet mнoжectbo bosmoжныx sнaчeний дpyгoй, t.e. иsmeнeниe oднoй иs beличин bлeчet иsmeнeниe ***pacnpeдeneнuя*** дpyгoй, b чactнoctи, moжet иsmeняtьcя ***cpeднee знaчe- нue*** дpyгoй.

*Mpuмep*. Ctatиctичecкoй яbляetcя sabиcиmoctь ypoжaйнoctи нe- кotopoй кyльtypы ot кoличectba bнocиmыx yдo6peний или кoличectba ocaдкob; sabиcиmoctь cпpoca нa tobap ot eгo цeны; нaдeжнoctи abto- mo6иля ot eгo bospacta и t. д.

Ctatиctичecкaя sabиcиmoctь bosникaet иs-sa toгo, чto нa sabи- cиmyю пepemeннyю bлияюt кaкиe-to нeyчteнныe или нeкoнtpoлиpye- mыe фaкtopы.

Пpи иsyчeнии ctatиctичecкoй sabиcиmoctи o6ычнo oгpaничи- baюtcя иccлeдobaниem ycpeднeннoй sabиcиmoctи: кaк b cpeднem 6yдet иsmeняtьcя sнaчeниe oднoй beличины пpи иsmeнeнии дpyгoй. Taкaя sabиcиmoctь нasыbaetcя ***pespeccuoннoŭ***. Бoлee ctpoгo, peгpeccиoннaя sabиcиmoctь meждy дbymя cлyчaйныmи beличинamи – эto фyнкциo- нaльнaя sabиcиmoctь meждy sнaчeнияmи oднoй иs ниx и ycлobныm ma- tematичecкиm oжидaниem дpyгoй.

Ocнobныm metoдom иccлeдobaния ctatиctичecкиx sabиcиmocteй яbляetcя ***кoppenяцuoннo***-***pespeccuoнныŭ*** aнaлиs.

***Кoppenяцuoнныŭ aнanuз*** coctoиt b oпpeдeлeнии ***cmeneнu cвязu***

meждy cлyчaйныmи beличинamи.

Цeлью ***pespeccuoннoso aнanuзa*** яbляetcя yctaнobлeниe ***фopnы зaвucunocmu*** meждy нa6людaemыmи beличинamи и oпpeдeлeниe пo экcпepиmeнtaльныm дaнныm ypabнeния sabиcиmoctи, кotopoe нasыba- юt ***выбopoчныn (snnupuчecкun) ypaвнeнuen pespeccuu***, a taкжe пpo- гнosиpobaниe c пomoщью ypabнeния peгpeccии cpeднeгo sнaчeния sa- bиcиmoй пepemeннoй пpи saдaннom sнaчeнии нesabиcиmoй пepemeн- нoй.

Bид эmпиpичecкoй фyнкции peгpeccии oпpeдeляюt иcxoдя иs:

1. coo6paжeний o фиsичecкoй cyщнoctи иccлeдyemoй sabиcиmoctи;
2. oпыta пpeдыдyщиx иccлeдobaний; 3) xapaкtepa pacпoлoжeния toчeк нa ***кoppenяцuoннon none***, кotopoe пoлyчaetcя, ecли otmetиtь нa плoc- кoctи bce toчки c кoopдинatamи (*xi, yi*), cootbetctbyющиe нa6людeни- яm.

Haи6oльший инtepec пpeдctabляet линeйнoe эmпиpичecкoe

ypabнeниe peгpeccии *y*  *ax*  *b* , t. к. 1) эto нaи6oлee пpoctoй cлyчaй

для pacчetob и aнaлиsa; 2) пpи нopmaльнom pacпpeдeлeнии фyнкция peгpeccии яbляetcя линeйнoй.

## 35. Выборочный коэффициент корреляции и его свойства.

Koличectbeннoй mepoй линeйнoй cbяsи meждy дbymя нa6людaemы- mи beличинamи cлyжиt ***выбopoчныŭ кosффuцueнm кoppenяцuu***.

*r*  *xy*  *x*  *y*

гдe

*x*  1 *n x* , *y*  1 *n*

*i*

*xy*  

*x y*

*y* , *xy*  1 *n x*  *y* - bы6opoчныe cpeдниe *x, y, xy*

*i*

*n i*1

*n*

*i i*

*i*1

*n i* 1

*x*2  *x* 2

*Dвy*

2

cootbetctbeннo, *x*  

*Dвx*

,  *y*  

, *x*2  1 *n*

*n i*1

*y*2   *y* 2



*x i* ,

*y*2  1 *n*



*n i* 1

*y*2 .

***Cвoŭcmвa выбopoчнoso кosффuцueнma кoppenяцuu.***

*i*

1. 1  *rxy*  1

1. Ecли

*rxy*

 1, to sнaчeния *x* и *y* cbяsaны линeйнoй sabиcиmoctью;

1. Ecли sнaчeния *x* и *y* нesabиcиmы, to

*rxy*

 0 .

1. Ecли *rxy*  0 , to c poctom oднoй beличины ybeличиbaetcя дpyгaя, ec-

ли *rxy*  0 , to, нao6opot, ymeньшaetcя.

***Mpoвepкa знaчunocmu кosффuцueнma кoppenяцuu*** - эto пpo-

bepкa toгo, чto кoэффициeнt кoppeляции sнaчиmo otличaetcя ot нyля.

T. к. bы6opкa пpoиsbeдeнa cлyчaйнo, нeльsя ytbepждatь, чto ecли bы-

6opoчный кoэффициeнt кoppeляции

*rxy*  0 , to и кoэффициeнt кoppe-

ляции гeнepaльнoй coboкyпнoctи

  0 . Эto sabиcиt ot cootнoшeния

o6ъema bы6opки и sнaчeния

*rxy*

. Ecли bы6opкa иs нopmaльнoгo pac-

пpeдeлeния, to пpobepкa пpoиsboдиtcя пo ***кpumepuю Cmbюдeнma***: ec- ли

*n*  2

1  *r*2

*xy*

*tpacu*

 *rxy*

* *tmaбz*

 *t* ,n2 ,

гдe

*t* ,n2

- кbaнtиль *t*-pacпpeдeлeния Ctьюдeнta (oпpeдeляetcя пo ta6-

лицe), to пpи saдaннom ypobнe sнaчиmoctи a (дoпycкaetcя, чto bыboд moжet 6ыtь oши6oчныm c нe6oльшoй bepoяtнoctью a) кoэффициeнt кoppeляции cчиtaetcя sнaчиmo otличaющиmcя ot нyля, a cлeдobateль- нo, cbяsь meждy beличинamи *x,y* пpиsнaetcя ctatиctичecки sнaчиmoй.

Пoдчepкнem, чto кoэффициeнt кoppeляции яbляetcя mepoй иmeннo *zuнeŭнoŭ* sabиcиmoctи. B cлyчae нeлинeйнoй sabиcиmoctи cbяsь meждy beличинoй кoэффициeнta кoppeляции и 6лиsoctью toчeк кoppeляциoннoгo пoля к нeкotopoй линии нe пpocлeжиbaetcя. Пoэto- my b пpaкtичecкиx saдaчax пpи bы6ope bидa эmпиpичecкoй фyнкции peгpeccии o6яsateльнo yчиtыbaюt xapaкtep pacпoлoжeния toчeк нa кoppeляциoннom пoлe.

36. Эмпирическое линейное уравнение регрессии. Метод наименьших квадратов.

Ocнobныm metoдom иccлeдobaния ctatиctичecкиx sabиcиmocteй

яbляetcя ***кoppenяцuoннo***-***pespeccuoнныŭ*** aнaлиs.

***Кoppenяцuoнныŭ aнanuз*** coctoиt b oпpeдeлeнии ***cmeneнu cвязu***

meждy cлyчaйныmи beличинamи.

Цeлью ***pespeccuoннoso aнanuзa*** яbляetcя yctaнobлeниe ***фopnы зaвucunocmu*** meждy нa6людaemыmи beличинamи и oпpeдeлeниe пo экcпepиmeнtaльныm дaнныm ypabнeния sabиcиmoctи, кotopoe нasыba- юt ***выбopoчныn (snnupuчecкun) ypaвнeнuen pespeccuu***, a taкжe пpo- гнosиpobaниe c пomoщью ypabнeния peгpeccии cpeднeгo sнaчeния sa- bиcиmoй пepemeннoй пpи saдaннom sнaчeнии нesabиcиmoй пepemeн- нoй.

Haи6oлee pacпpoctpaнeнныm metoдom нaxoждeния кoэффициeн-

tob эmпиpичecкoгo ypabнeния peгpeccии

*y*ˆ  *ax*  *b*

пo bы6opкe

(*x* , *y* ),

1,...,

яbляetcя ***nemoд нauneнbuux квaдpamoв (MHК)***. Cytь

эtoгo metoдa b tom, чto кoэффициeнtы *a* и *b* bы6иpaюt taк, чto6ы

cymma кbaдpatob otклoнeний нa6людaemыx sнaчeний *yi* ot пpeдcкasы-

baemыx пo ypabнeнию *y*ˆ*i*  *axi*  *b* 6ылa mиниmaльнoй. Taкиm o6pa-

som, mиниmиsиpyetcя фyнкция

*Q* (*a*,*b*) 

*n* ( *y*  \_

*n*

 ( *y*

* *b*  *ax* )2  min .

# 

*i*1

*i yi* )

 *i i*

*i* 1

*a*,*b*

Heo6xoдиmыm ycлobиem cyщectbobaния mиниmyma дaннoй фyнкции дbyx пepemeнныx яbляetcя pabeнctbo нyлю ee чactныx пpo-

иsboдныx пo нeиsbectныm пapametpam *b*, *a* :

*Q*   2 *n*

( *y*  *b*  *a x* )  0,

 *b*



 *i i*

*i*1 .

*Q*   2 *n*

( *y*  *b*  *a x* ) *x*

 0.

 *a*



*i*1

*i i i*

Otcюдa пoлyчaem ***cucmeny нopnanbныx ypaвнeнuŭ***:

*nb*  *a*  *xi*



  *yi* ,

2

*b*  *xi*  *a*  *xi*   *xi yi* .

Metoд нaиmeньшиx кbaдpatob шиpoкo пpиmeняetcя пpи ctatиctи- чecкoй o6pa6otкe pesyльtatob иsmepeний.

## Простые и составные числа. Бесконечность множества простых чисел. Простые числа Мерсенна. Задача факторизации целых чисел.

***Mнoжecmвo цenыx чucen*** o6osнaчaюt

**Z** = {0; 1; 2; …; *n*; …}.

Hatypaльныmи нasыbaюtcя чиcлa, кotopыe иcпoльsyюtcя пpи cчete; ***nнoжecmвo нamypanbныx чucen*** o6osнaчaюt

**Æ** = {1; 2; …; *n*; …}.

Ha mнoжectbe цeлыx чиceл oпpeдeлeны oпepaции cлoжeния и ymнoжeния, a taкжe oпepaция bычиtaния кaк o6patнaя к oпepaции cлoжeния. Cymma, pasнoctь и пpoиsbeдeниe дbyx цeлыx чиceл bce-

гдa яbляюtcя цeлыm чиcлom. Pesyльtat дeлeния дbyx цeлыx чиceл нe bceгдa яbляetcя цeлыm чиcлom.

**Oпp. 1.** Ecли для цeлыx чиceл *a* и *b*, гдe *b*  0, cyщectbyюt цe- лыe чиcлa *q* и *r* taкиe, чto

*a*  *b*  *q*  *r*, гдe 0  *r*  *b* ,

to *r* нasыbaюt ***ocmamкon***, a *q* – ***чacmныn*** (***нenonныn чacmныn***

пpи *r*  0 ) ot дeлeния *a* нa *b*.

**T 1 (o дeлeнnn c octatкoм).** Для лю6ыx цeлыx чиceл *a* и *b*,

гдe *b*  0, cyщectbyюt eдинctbeнныe цeлыe чиcлa *q* и *r* taкиe, чto

**Пpnмep 1.**

*a*  *b*  *q*  *r*,

гдe 0  *r*  *b* .

**1)** *a*  37, *b*  15. Пocкoлькy 37  15  2  7, to *q*  2, *r*  7.

**2)** *a*  26, *b*  4. Пocкoлькy 26  4  (7)  2, to *q*  7, *r*  2.

**3)** *a*  22, *b*  5. Пocкoлькy 22  5  (4)  2, to *q*  4, *r*  2.

**4)** *a*  15, *b*  6. Пocкoлькy 15  6  3  3, to *q*  3, *r*  3. 

**Oпp. 2.** Ecли octatoк ot дeлeния *a* нa *b* pabeн 0 ( *r*  0 ), t. e.

*a*  *b*  *q*, to гobopяt,

* чto *a* ***дenumcя нa*** *b* ***u нa*** *q* (и пишyt *a*⁝*b*, *a*⁝*q* );
* чto *a* яbляetcя ***кpamныn*** чиceл *b* и *q*;
* чto *b* и *q* ***дenяm*** *a* (и пишyt *b a*, *q a* );
* чto *b* и *q* яbляюtcя ***дenumenяnu*** (или ***nнoжumenяnu***) чиcлa *a*.

Бyдem o6osнaчatь *b* | *a*,

ecли *b* нe дeлиt *a*.

Чиcлo 0 дeлиtcя нa лю6oe цeлoe чиcлo *b*  0.

Лю6oe цeлoe чиcлo *a*  0 дeлиtcя нa 1; 1; *a*;  *a*.

B дaльнeй-

шem 6yдem гobopиtь toлькo o *цezыx nozoжumezbныx*, t. e. *нamy- pazbныx дezumezяx*.

**Пpoctыe n coctabныe uncлa**

**Oпp. 3.** Hatypaльнoe чиcлo

*n*  1

нasыbaetcя ***npocmыn***, ecли

oнo дeлиtcя toлькo нa 1 и нa camo ce6я, b пpotиbнom cлyчae *n*

нasыbaetcя ***cocmaвныn***.

Для цeлeй кpипtoгpaфии (кaк для пpaкtичecкoй peaлиsaции и o6ocнobaния ctoйкoctи кpипtoгpaфичecкиx cpeдctb, taк и для pas- pa6otки metoдob иx bcкpыtия) нeo6xoдиmo paspa6atыbatь эффeк- tиbныe metoды и aлгopиtmы:

* пpobepки пpoctotы цeлыx чиceл;
* пoиcкa 6oльшиx пpoctыx чиceл (b кpипtoгpaфии иcпoльsy- юtcя 6oльшиe пpoctыe чиcлa длинoй 6oлee 80–90 дecяtичныx sнa- кob);
* фaкtopиsaции цeлыx чиceл.

***Øaкmopuзaцueŭ*** нatypaльнoгo чиcлa нasыbaetcя pasлoжeниe эtoгo чиcлa b пpoиsbeдeниe пpoctыx comнoжиteлeй. Эta saдaчa иmeet 6oльшyю bычиcлиteльнyю cлoжнoctь. Oдин иs camыx пo- пyляpныx metoдob кpипtoгpaфии c otкpыtыm ключom, metoд RSA, ocнobaн нa tpyдoemкoctи saдaчи фaкtopиsaции длинныx цeлыx чиceл.

**Чncлa Mepceннa**

***1ucna Mepceннa*** – эto чиcлa bидa 2 *p*  1.

Чиcлa Mepceннa 6ыли

otкpыtы b pesyльtate пoиcкa cobepшeнныx чиceл (***coвepueнныnu*** нasыbaюt- cя нatypaльныe чиcлa, кotopыe pabны cymme bcex cboиx дeлиteлeй, meньшиx дaннoгo чиcлa, нaпpиmep, 6 = 1 + 2 + 3; пepbыe чetыpe cobepшeнныx чиcлa – эto 6; 28; 496; 8128).

Oдниm иs cboйctb чиceл Mepceннa яbляetcя to, чto чиcлa taкoгo bидa moгyt 6ыtь пpoctыmи toлькo toгдa, кoгдa *p* – пpoctoe чиcлo. Oднaкo нe для

лю6oгo пpoctoгo *p* чиcлo 2*p*  1

яbляetcя пpoctыm, нaпpиmep,

## 211 – 1 

2047

##  23  89.

1. НОД и НОК целых чисел. Основная теорема арифметики. Методы нахождения НОД.

**Oпp. 1.** Maкcиmaльный иs o6щиx дeлиteлeй цeлыx чиceл

*a*1, *a*2 ,…, *an*

нasыbaetcя иx ***нauбonbuun oбщun дenumenen***

(***HOД***) и o6osнaчaetcя: HOД (*a*1, *a*2 ,…, *an* ) или (*a*1, *a*2 ,…, *an* ).

**Oпp. 2.** Mиниmaльнoe нatypaльнoe иs o6щиx кpatныx цeлыx

чиceл

*a*1, *a*2 ,…, *an*

нasыbaetcя иx ***нauneнbuun oбщun кpamныn***

(***HOК***) и o6osнaчaetcя: HOK (*a*1, *a*2 ,…, *an* ) или [*a*1, *a*2 ,…, *an* ].

**Уtb. 1.** Ecли кaнoничecкиe pasлoжeния дbyx чиceл иmeюt bид

*a*  *p*1 *p*2 ... *p**s* ,

*b*  *p*1 *p*2 ... *p**s* , гдe  ,   0,

1 2 *s*

to

1 2 *s i i*

(*a*,*b*)  *p*1 *p*2 ... *p**s* , гдe   min{ ,  };

1 2 *s i i i*

[*a*,*b*]  *p*1 *p*2 ... *p**s* , гдe   max{ ,  }.

1 2 *s i i i*

**Пpnмep 1.** Haйдem (168,180) и [168,180].

*Peneнue.* Пocкoлькy

168  2  84  2  2  42  2  2  2  21  2  2  2  3 7  23  3 7;

180  2  90  2  2  45  2  2  315  2  2  3  3 5  22  32  5,

to

(168,180)  22  31  50  70  12;

[168,180]  23  32  51  71  2520. 

**T 1.** HOK и HOД дbyx цeлыx чиceл cbяsaны cootнoшeниem:

[*a*,*b*](*a*,*b*)  *ab*.

*Дoкaзamezbcmвo*. Ecли

(*a*1,*b*1)  1. Toгдa

*d*  (*a*,*b*),

to *a*  *a*1*d* ,

*b*  *b*1*d* ,

гдe

[*a*,*b*]  *a b d*  *ab* 

*ab* ,

1 1

чto и дoкasыbaet teopemy. a

*d* (*a*,*b*)

**Oпp. 3.** Цeлыe чиcлa *a* и *b* нasыbaюtcя ***взaunнo npocmыnu***,

ecли (*a*,*b*)  1. (Дpyгиmи cлobamи, эto чиcлa, нe иmeющиe o6щиx

пpoctыx дeлиteлeй.)

**Пpnмep 2.** Чиcлa 6 и 35 bsaиmнo пpoctы, taк кaк (6,35) = 1, нo 6 и 27 нe яbляюtcя bsaиmнo пpoctыmи, taк кaк (6,27) = 3. 

*Эaмeuaнue.* Чиcлo 1 bsaиmнo пpocto c лю6ыm цeлыm чиcлom; чиcлo 0 bsaиmнo пpocto toлькo c 1 и 1.

**T 2.** Ecли *a*  *bq*  *r*, to (*a*,*b*)  (*b*, *r*).

*Дoкaзamezbcmвo*. Пyctь (*a*,*b*)  *d*, (*b*,*r*)  *k*.

Пo cboйctby дeлиmoctи, ecли *d a* и teльнo, *d k* .

*d b*, to

*d r* .

Cлeдoba-

*k d* .

C дpyгoй ctopoны, ecли *k b* и

*k r* , to

*k a*.

Cлeдobateльнo,

Пocкoлькy *d k* и кasaнa. a

*k d* ,

пpичem *d*, *k*  0, to *d*  *k*

и teopema дo-

Ha эtoй teopeme ocнobыbaetcя aлгopиtm Ebклидa.

**T 3 (Ocнobнaя teopeмa apnøмetnкn).** Bcякoe нatypaльнoe

чиcлo

*n*  1

oднosнaчнo pacклaдыbaetcя b пpoиsbeдeниe пpoctыx

чиceл c toчнoctью дo пopядкa cлeдobaния mнoжиteлeй:

*n*  *p*1 *p*2 … *ps* .

Ecли b pasлoжeнии нatypaльнoгo чиcлa нa пpoctыe mнoжиteли co6patь oдинaкobыe mнoжиteли, to пoлyчиm ***кaнoнuчecкoe paз- noжeнue*** нatypaльнoгo чиcлa:

*n*  *p r*1 *p r*2 … *p rt* .

1 2 *t*

Kaнoничecкиm pasлoжeниem цeлoгo otpицateльнoгo чиcлa

*z*  *n*

cчиtaetcя, cootbetctbeннo, eгo пpeдctabлeниe b bидe

*z*  *pr*1 ... *prt* .

1 *t*

## Алгоритм Евклида. Расширенный алгоритм Евклида. Соотношение Безу.

***Ansopumn Eвкnuдa*** – aлгopиtm для oпpeдeлeния HOД дbyx чиceл пytem пocлeдobateльнoгo пpиmeнeния teopemы o дeлeнии c octatkom.

**T 3.** Haи6oльший o6щий дeлиteль цeлыx чиceл *a* и *b* (гдe

*a* | *b*, *b* | *a*, *a*  *b* ) pabeн пocлeднemy otличнomy ot нyля octatky

ot дeлeния b цeпoчke pabeнctb:

*a*  *bq*1  *r*1;

*b*  *r*1*q*2  *r*2 ,

ecли

*r*1  0;

…;

*rn*2  *rn*1*qn*  *rn* , ecли

*rn*1  0;

t. e.

*rn*  (*a*,*b*).

*rn*1  *rnqn*1,

ecли

*rn*  0,

*Дoкaзamezbcmвo*. Coглacнo teopeme 2 и пocкoлькy octatoк ot дeлeния, иmeem

(*a*,*b*)  (*b*, *r*1 )  (*r*1, *r*2 )  ...  (*rn*1, *rn* )  *rn* .

*rn*  0

кaк

Пpoцecc пoлyчeния (*a*,*b*) кoнeчeн, пocкoлькy mы oпepиpyem

toлькo c цeлыmи чиcлamи и, нaчинaя c дeлeния *r*1 нa *r*2, – c цeлыmи пoлoжиteльныmи чиcлamи. Пpи эtom идet пoctoяннoe ymeньшeниe

octatкob

*ri* : 0  *ri*  *ri*1 , пoэtomy sa кoнeчнoe чиcлo шaгob 6yдet дo-

ctигнyt octatoк *rn*1  0. a

**Oпp. 4.** Пoлyчeннoe pabeнctbo нasыbaюt ***nuнeŭныn paзnoжe- нuen,*** или ***coomнoueнuen Бeзy*** для нaи6oльшeгo o6щeгo дeлиteля цeлыx чиceл *a* и *b*, a чиcлa *u* и *v* – ***кosффuцueнmanu Бeзy***.

**Пpnмep 4.** Haйдem cootнoшeниe Бesy для (72, 26)*. Peneнue*. Иs пpиmepa 3 cлeдyet, чto

2 = 20 + 6 (–3) =

= 20 + (26 + 20 (–1))  (–3) =

= 20  4 + 26 (–3) =

= (72 + 26 (–2)) 4 +26 (–3) =

= 72  4 + 26 (–11).

Taкиm o6pasom, 2 = 72*u* + 26*v*, гдe *u* = 4, *v* = –11.

*Эaмeuaнue.* Чиcлa *u* и *v* нe яbляюtcя eдинctbeннoй пapoй c ta- киm ycлobиem. Эto cлeдyet иs teopии диoфaнtobыx линeйныx ypabнeний, кotopaя 6yдet paccmotpeнa нижe. Taк, b пpиmepe 4 чиcлa *u* = –9 и *v* = 25 taкжe yдobлetbopяюt cootнoшeнию Бesy.

**Cлeдctbne teopeмы 4 (кpntepnй bзanмнoй пpoctotы).** Цe- лыe чиcлa *a* и *b* bsaиmнo пpoctы toгдa и toлькo toгдa, кoгдa cyщe- ctbyюt taкиe цeлыe *u* и *v*, чto

*au*  *bv*  1.

*Дoкaзamezbcmвo.* )

Ecли (*a*,*b*)  1,

to иs cootнoшeния Бesy

cлeдyet, чto cyщectbyюt taкиe цeлыe чиcлa *u* и *v*, чto *au*  *bv*  1.

) O6patнo, пyctь cyщectbyюt taкиe цeлыe *u* и *v*, чto

*au*  *bv*  1.

Ecли (*a*,*b*)  *d*  1,

to *d* 1

(пo cboйctby дeлиmoctи), a

sнaчиt, (*a*,*b*) 1. a

### Pacнnpeнный aлгopntм Ebклnдa

Пpи нaxoждeнии cootнoшeния Бesy 6oлee yдo6eн ***pacuupeн- ныŭ*** (***oбoбщeнныŭ***) ***ansopumn Eвкnuдa***, пosboляющий bычиcляtь кoэффициeнtы Бesy пapaллeльнo c нaxoждeниem HOД.

Пyctь | *a* || *b* | . Пoлoжиm

*u*0  1,

*u*1  0,

*v*0  0,

*v*1  1,

*r*0  *a*; *r*1  *b*.

Дaлee пocлeдobateльнo bычиcляem:

*ui*1  *ui*1  *qiui* ,

*vi*1  *vi*1  *qivi* ,

*ri*1  *ri*1  *qi ri* ,

гдe *qi* – нeпoлнoe чactнoe ot дeлeния *ri*1 нa *ri* .

Pa6ota aлгopиtma saкaнчиbaetcя, ecли нa нeкotopom шaгe *ri*1  0. Пpи эtom нa пpeдыдyщem шaгe нaйдeны HOД и кoэффици- eнtы Бesy:

(*a*,*b*)  *ri* ,

*u*  *ui* ,

*v*  *vi* .

O6ocнobaниem aлгopиtma cлyжиt cлeдyющaя teopema. **T 5.** Пpи bcex *i* bыпoлняetcя pabeнctbo: *uia + vib = ri*. *Дoкaзamezbcmвo* пpoboдиtcя индyкциeй пo *i.*

1. *Бaзa uндyкцuu*: ecли *i* = 0 или *i* = 1, to, oчebиднo, pabeнctbo bыпoлняetcя:

1 *a*  0  *b*  *a*;

0  *a*  1 *b*  *b*.

1. *Шas uндyкцuu.* Пpeдпoлoжиm, чto ytbepждeниe bepнo для bcex *k*  *i*. Toгдa для cлeдyющeгo нomepa *i* + 1 пoлyчиm

*ui*1  *a*  *vi*1  *b*  (*ui*1  *qiui* )  *a*  (*vi*1  *qivi* )  *b* 

 (*ui*1  *a*  *vi*1  *b*)  *qi*  (*ui*  *a*  *vi*  *b*)  *ri*1  *qi*  *ri*  *ri*1,

чto и tpe6obaлocь дoкasatь. a

## Диофантовы линейные уравнения.

**Oпp. 5. *Дuoфaнmoвыn nuнeŭныn ypaвнeнuen*** c дbymя нeиs- bectныmи нasыbaetcя ypabнeниe bидa

гдe

*a*, *b*, *c* **Z**,

*a*, *b*  0,

*ax*  *by*  *c*,

peшeния (*x*; *y*)

(1)

ищytcя b цeлыx чиcлax.

Иныm cлobamи, bce кoэффициeнtы и нeиsbectныe – цeлыe чиcлa.

**T 6.** Ypabнeниe (1) paspeшиmo b цeлыx чиcлax toгдa и toлькo toгдa, кoгдa (*a*, *b*) *c*.

*Дoкaзamezbcmвo*. 1) *Heoбxoдuмocmb*. Пyctь

( *x*0 ; *y*0 )

* цeлo-

чиcлeннoe peшeниe ypabнeния (1). Toгдa cпpabeдлиbo pabeнctbo

*ax*0  *by*0  *c*,

(*a*, *b*) *c*.

a sнaчиt, пo cboйctby дeлиmoctи цeлыx чиceл

2) *Дocmamouнocmb*. Пyctь

*d*  (*a*, *b*)

и *d c*,

toгдa *c*  *dt*

для

нeкotopoгo

*t*  **Z**.

Зaпишem cootнoшeниe Бesy для

*d*  (*a*, *b*) :

cy-

щectbyюt taкиe чиcлa *u*, *v*  **Z**,

чto

*au*  *bv*  *d*.

Ymнoжaя пocлeд-

нee pabeнctbo нa *t*, пoлyчaem

*aut*  *bvt*  *c*,

t. e. (*tu*; *tv*)

* цeлoчиc-

лeннoe peшeниe ypabнeния (1).a

**T 7.** Ypabнeниe (1) ли6o нe иmeet peшeний b цeлыx чиcлax, ли6o иmeet 6ecкoнeчнo mнoгo peшeний b цeлыx чиcлax.

*Дoкaзamezbcmвo*. Ecли (*a*, *b*) | *c*, to b cилy teopemы 6 ypabнe-

ниe (1) нe иmeet peшeний b цeлыx чиcлax.

Ecли (*a*, *b*) *c*, to ypabнeниe (1) paspeшиmo. Пpи эtom ecли

( *x*0 ; *y*0 ) – oднo иs peшeний ypabнeния (1), t. e. *ax*0  *by*0  *c*, to пpи

пpoиsboльнom цeлom *t* cпpabeдлиbo

*a*(*x*0  *bt*)  *b*( *y*0  *at*)  *c*,

a sнaчиt,

( *x*0  *bt*; *y*0  *at*)

taкжe яbляetcя peшeниem ypabнeния (1)

пpи bcex *t*  **Z**. a

Moжнo пoкasatь, чto иmeя oднo peшeниe

( *x*0 ; *y*0 )

ypabнeния

1. , moжнo пoлyчиtь bce eгo peшeния пo фopmyлe

 *x*  *b t*; *y*  *a t*  ,

гдe *d*  (*a*, *b*),

*t*  **Z**. Пpи эtom чactнoe peшeниe

 0 *d* 0 *d* 

 

( *x*0 ; *y*0 )

(*a*, *b*).

moжet 6ыtь нaйдeнo c пomoщью cootнoшeния Бesy для

### Aлгopntм peнeнnя дnoøaнtoba лnнeйнoгo ypabнeнnя (1).

* 1. Ecли (*a*,*b*) | *c*, to ypabнeниe (1) нe иmeet peшeний b цeлыx чиcлax.
  2. Ecли (*a*, *b*)  *d*,

*d* | *c*,

to пoлyчaem (нaпpиmep, c пomoщью

pacшиpeннoгo aлгopиtma Ebклидa) cootнoшeниe Бesy для (*a*, *b*) и нaxoдиm taкиe чиcлa *u*0 , *v*0  **Z**, чto

*au*0  *bv*0  *d*.

* 1. Ymнoжиb o6e чactи pabeнctba (2) нa

*a d u*0  *b d v*0  *c*,

*c c*

*c* , пoлyчиm

*d*

a sнaчиt, *x*  *c u* , *y*  *c v*

* чactнoe peшeниe ypabнeния (1).

0 *d* 0 0 *d* 0

**4.** Mнoжectbo цeлoчиcлeнныx peшeний ypabнeния (1) saдaetcя фopmyлoй

 *x*

* *b t*; *y*
* *a t* 



*t*  **Z** .

 0 *d* 0 *d*  

  

## Понятие сравнимости по модулю m. Арифметические свойства сравнений. Множество классов вычетов.

**T 1.** Пyctь *m* – нatypaльнoe чиcлo. Для лю6ыx цeлыx чиceл *a* и

*b* cлeдyющиe ycлobия pabнocильны:

* 1. *a* и *b* иmeюt oдинaкobыe octatки ot дeлeния нa *m*;
  2. *a*  *b* дeлиtcя нa *m*, t. e. *a*  *b*  *mq* для пoдxoдящeгo цeлo- гo *q*;
  3. *a* = *b* + *mq* для нeкotopoгo цeлoгo *q*.

*Дoкaзamezbcmвo* пpoboдиtcя пo cxeme 1)  2)  3) 1).

1)  2).

Пyctь

*a*  *q*1*m*  *r*, *b*  *q*2*m*  *r*,

гдe 0  *r*  *m*.

Toгдa

*a*  *b*  *q*1*m*  *q*2*m*  (*q*1  *q*2 )*m*, t. e. *a*  *b* дeлиtcя нa *m*.

2)  3). Ecли *a*  *b* дeлиtcя нa *m*, t. e. *a*  *b*  *mq*

для нeкoto-

poгo *q* **Z**, to *a*  *b*  *mq*.

3)  1). Пyctь *a*  *q*1*m*  *r*1, *b*  *q*2*m*  *r*2 , 0  *r*1, *r*2  *m*.

Дoкaжem,

чto ecли *a*  *b*  *mq*, to *r*1  *r*2 .

Пoдctabляя b эto cootнoшeниe bыpaжeния для *a* и *b*, пoлyчиm

*q*1*m*  *r*1  *q*2*m*  *r*2  *mq*,

otкyдa

*r*1  *r*2  (*q*2  *q*  *q*1)*m*,

t. e.

*m r*1  *r*2.

Ho пocкoлькy 0  *r*1, *r*2  *m*, to *r*1  *r*2 . a

**Oпp. 1.** Цeлыe чиcлa *a* и *b* нasыbaюtcя ***cpaвнunыnu no noдy- nю*** *m*, ecли oни yдobлetbopяюt oднomy иs ycлobий teopemы 1. Эtot фaкt o6osнaчaюt фopmyлoй *a*  *b*(mod *m*).

Иtaк,

*a* = *b* + *mq* для нeкo- topoгo *q*  **Z**

*a* и *b* иmeюt oдинaкobыe octatки ot дe- лeния нa *m*

*a*  *b*(mod *m*) 

 *a*  *b*⁝*m* 

**Apnøмetnuecкne cboйctba cpabнeнnй**

1. B cpabнeнии moжнo ot6pacыbatь или дo6abляtь cлaгaemыe, дeлящиecя нa moдyль: ecли *a*  *b*(mod *m*), to для bcякoгo *k*  **Z**

*a*  (*b*  *km*)(mod *m*).

1. Cpabнeния moжнo пoчлeннo cклaдыbatь, bычиtatь, ymнo- жatь, bosboдиtь b нatypaльнyю cteпeнь:

ecли *a*  *b*(mod *m*), *c*  *d* (mod *m*), to

(*a*  *c*)  (*b*  *d* )(mod *m*); *ac*  *bd* (mod *m*);

*an*  *bn* (mod *m*) пpи лю6om *n*  **Æ**.

*Дoкaзamezbcmвo.* Дoкaжem btopoe cootнoшeниe (cpabнeния

moжнo пoчлeннo ymнoжatь). Ecли *a*  *b*(mod *m*), *c*  *d* (mod *m*), to

*a*  *b*  *mq*1, *c*  *d*  *mq*2 . Toгдa

*ac*  (*b*  *mq*1)(*d*  *mq*2 )  *bd*  *mq*1*d*  *mq*2*b*  *m*2*q*1*q*2  *bd*  *mt*, *t*  **Z**.

Cлeдobateльнo, *ac*  *bd* (mod *m*). a

*Уnpaжнeнue*. Дoкasatь пepboe cootнoшeниe.

1. K o6eиm чactяm cpabнeния moжнo пpи6abиtь или bычectь oднo и to жe чиcлo; o6e чactи cpabнeния moжнo ymнoжиtь нa oднo и to жe чиcлo:

ecли *a*  *b*(mod *m*), to для bcякoгo *c*  **Z**

(*a*  *c*)  (*b*  *c*)(mod *m*); *ac*  *bc*(mod *m*).

1. Cpabнeниe moжнo coкpatиtь нa o6щий mнoжиteль, bsaиmнo пpoctoй c moдyлem: пyctь *a*  *a*1*d* , *b*  *b*1*d* , (*d*, *m*) = 1, toгдa

ecли *a*1*d*  *b*1*d* (mod *m*), to *a*1  *b*1(mod *m*).

*Дoкaзamezbcmвo.* Дeйctbиteльнo,

*a*1*d*  *b*1*d* (mod *m*)

 (*a*1*d*  *b*1*d* )⁝*m* 

*d* (*a*1  *b*1)⁝*m*,

otкyдa, пocкoлькy *d* и *m* bsaиmнo пpoctы, cлeдyet (*a*1  *b*1)⁝*m*, t. e.

*a*1  *b*1(mod *m*). a

1. Ecли b cpabнeнии *a*  *b*(mod *m*) чиcлa *a*, *b*, *m* иmeюt o6щий mнoжиteль *d*, to нa нeгo cpabнeниe moжнo coкpatиtь:

*a*  *b*  mod *m* .

*d d*  *d* 

 

*Дoкaзamezbcmвo.* Cpabнeниe

*a*  *b*(mod *m*)

pabнocильнo

*a*  *b*  *mq* пpи нeкotopom *q* **Z**. Toгдa, taк кaк чиcлa *a*, *b* и *m* дe-

ляtcя нa *d*, to *a*  *b*  *m q*  *a*  *b*  mod *m* . a

*d d d d d*  *d* 

 

*a*  *b*(mod *m*1),

**6.** 

...,

 *a*  *b*(mod[*m* ,...,*m* ]).

 1 *k*

*a*  *b*(mod *mk* )



*Дoкaзamezbcmвo.* Cpabнeниe

*a*  *b*(mod *mi* )

osнaчaet, чto

(*a*  *b*)⁝*mi* ; yкasaннaя cиctema cpabнeний osнaчaet, чto чиcлo *a*  *b* дeлиtcя нa кaждoe *mi* ,1  *i*  *k*, a sнaчиt *a*  *b* дeлиtcя нa HOK чи- ceл *mi* ,1  *i*  *k*, t. e. (*a*  *b*)⁝[*m*1,..., *mk* ]  *a*  *b*(mod[*m*1,..., *mk* ]). a

**7.** Ecли *a*  *b*(mod *m*), to (*a*, *m*) = (*b*, *m*).

*Дoкaзamezbcmвo.* Cpabнeниe *a*  *b*(mod *m*) pabнocильнo pabeн- ctby *a*  *b*  *mq* пpи нeкotopom *q* **Z**.

Toгдa ecли *d a*, *d m*, to *d b*; ecли *d b*, *d m*, to *d a*, t. e. bcя-

кий дeлиteль чиceл *a* и *m* яbляetcя дeлиteлem чиcлa *b*, и bcякий дeлиteль чиceл *b* и *m* яbляetcя дeлиteлem чиcлa *a*, a cлeдobateльнo, (*a*, *m*) = (*b*, *m*).a

Инoгдa пoлesнo иmetь b bидy cлeдyющee ytbepждeниe, o6o6- щaющee и ytoчняющee cboйctba 3, 4 и 5.

**Уtb. 1.**

1. Пpи лю6om нatypaльнom *c*  0

*a*  *b*(mod *m*) 

1. Ecли (*c*, *m*) = 1, to

*a*  *b*(mod *m*) 

*ac*  *bc*(mod *mc*).

*ac*  *bc*(mod *m*).

**Oпp. 2.** Mнoжectbo bcex чиceл, cpabниmыx c *a* пo moдyлю *m*, нasыbaetcя ***кnaccon вычemoв no noдynю*** *m* (пo-лatинcки

«residua» – «octatoк, octabшaяcя чactь») и o6osнaчaetcя *a* , t. e.

*a*  *b*  **Z** : *b*  *a*(mod *m*),

или

*a* ...; *a*  2*m*; *a*  *m*; *a*; *a*  *m*; *a*  2*m*;....

Лю6oe чиcлo иs клacca bычetob нasыbaюt ***вычemon***. Пpи o6o-

sнaчeнии клacca bычetob moжнo иcпoльsobatь лю6oй элemeнt клacca, пocкoлькy кaждый пpeдctabиteль клacca oднosнaчнo oпpe-

дeляet cboй клacc, t. e. для лю6oгo чиcлa *b* *a* клacc *b*  *a*.

**Уtb. 2.** *a*  *b*(mod *m*)  *a*  *b*.

tob.

**Уtb. 3.** Pasличныe клaccы bычetob нe иmeюt o6щиx элemeн-

### Mнoжectbo клaccob bыuetob

Пpи дeлeнии цeлыx чиceл нa нatypaльнoe чиcлo *m* cyщectbyet

pobнo *m* pasличныx octatкob: 0, 1, ..., *m*  1.

Cootbetctbeннo эtиm

octatкam mнoжectbo цeлыx чиceл **Z** pas6иbaetcя нa *m* нeпepece- кaющиxcя клaccob bычetob пo moдyлю *m*. B cootbetctbии c octat- кom ot дeлeния нa *m* эtи клaccы o6osнaчaюtcя 0, 1, ..., *m*  1.

**Oпp. 3.** Mнoжectbo bcex клaccob cpabниmыx дpyг c дpyгom чи- ceл пo moдyлю *m* нasыbaюt ***nнoжecmвon кnaccoв вычemoв no noдynю*** *m* и o6osнaчaюt чepes **Z** /*m***Z** или **Z** *m* :

**Z***m*  **Z** /*m***Z**  0; 1; ...; *m* 1.

Taкиm o6pasom, **Z** *m* – mнoжectbo иs *m* элemeнtob.

**Пpnмep 2. Z**7  **Z** /7**Z**  0; 1; 2; 3; 4; 5; 6. 

Ha mнoжectbe **Z** *m*

клaccob bычetob пo saдaннomy moдyлю

moжнo bbectи apифmetичecкиe oпepaции cлoжeния, bычиtaния и ymнoжeния.

**Oпp. 4. *Cynnoŭ*** клaccob bычetob

*a*, *b* **Z***m*

нasыbaetcя клacc

*a*  *b*  *a*  *b*;

***paзнocmbю*** клaccob bычetob

*a*  **Z** *m*

и *b* **Z***m*

нasы-

baetcя клacc

*a*  *b*  *a*  *b*;

***npouзвeдeнuen*** клaccob bычetob

*a*, *b* **Z***m*

нasыbaetcя клacc

*a*  *b*  *a*  *b*.

## Функция Эйлера. Теорема Эйлера. Малая теорема Ферма.

**Oпp. 1. *Øyнкцuя 5ŭnepa*** (*m*) ctabиt b cootbetctbиe кaждomy

нatypaльнomy

*m*  1 кoличectbo нatypaльныx чиceл, нe пpebocxo-

дящиx *m* и bsaиmнo пpoctыx c *m*.

Пo oпpeдeлeнию пoлaгaetcя (1) = 1.

**Пpnмep 1.** (2) = 1; (3) = 2; (4) = 2; (5) = 4; (6) = 2; (7) = 6.

**T 1 (o bыuncлeнnn знaueнnй øyнкцnn 7йлepa).**

* 1. ( *p*)  *p* 1 для кaждoгo пpoctoгo чиcлa *p*;
  2. ( *ps* )  *ps*1( *p* 1), ecли *p* – пpoctoe чиcлo;

**3)** ecли (*m*, *n*) = 1, to (*mn*) = (*m*)(*n*);

1. ecли *m*  *p s*1 *p s*2 … *p st*

* кaнoничecкoe pasлoжeниe чиcлa *m*,

1 2 *t*

to



(*m*)  *p* ( *p* 1) *p* ( *p* 1)… *p* ( *p* 1).

*s* 1

1

*s* 1

2

*s* 1

*t*

1 1

2

2

*t*

*t*

### T 2 [7йлep, 1760]. Для

*m***Æ**, *m* 1, *a* **Z**

(*a*, *m*)  1  *a*(*m*)  1(mod *m*).

*Дoкaзamezbcmвo.* )

Пyctь

*x*1, *x*2 , ..., *x*( *m* )

* пpиbeдeннaя cи-

ctema bычetob пo moдyлю *m*. B cилy ytbepждeния 2 пpи (*a*,*m*)  1

чиcлa

*ax*1, *ax*2 , ..., *ax*( *m* )

taкжe o6pasyюt пpиbeдeннyю cиctemy bы-

чetob пo moдyлю *m*. Yctaнobиm bsaиmнo oднosнaчнoe cootbetctbиe meждy эtиmи дbymя cиctemamи, пoctabиb кaждomy иs чиceл

*ax*1, *ax*2 , ..., *ax*(*m* )

taк, чto

cpabниmoe c ниm чиcлo иs cиctemы

*ax*1  *x* (mod *m*),

*ax*2  *x* (mod *m*),

…,

*ax*( *m* )  *x* (mod *m*),

*x*1, *x*2 , ..., *x*( *m* )

гдe

*x* , *x* , ..., *x* – эto нeкotopыm o6pasom пepectabлeнныe чиcлa

*x*1, *x*2 , ..., *x*( *m* ).

Пepemнoжиb bce эtи cpabнeния, пoлyчиm

*a*(*m*)*x*1*x*2...*x*(*m*)  *x**x*...*x* (mod*m*),

пpичem

*x* *x*...*x*  *x*1 *x*2 ...*x*( *m* ) ,

пocкoлькy эto te жe чиcлa, нeкoto-

pыm o6pasom пepectabлeнныe. Пocкoлькy кaждoe иs чиceл

*x*1, *x*2 , ..., *x*( *m* )

bsaиmнo пpocto c *m*, to и иx пpoиsbeдeниe bsaиmнo

пpocto c *m*. Пoэtomy пoлyчeннoe cpabнeниe moжнo coкpatиtь нa

пpoиsbeдeниe

*x*1*x*2 ...*x*( *m* )  *x* *x*...*x* ,

чto пpиboдиt к cpabнeнию

*a*(*m*)  1(mod *m*).

) Пocкoлькy

## (*m*)  1,

to иs

*a*(*m*)  1(mod *m*)

cлeдyet, чto

*a*  *a*(*m*)1  1,

a sнaчиt, *a* – o6patиmый элemeнt b **Z**

*m*. Otcюдa b cи-

лy teopemы 2 §3 saключaem, чto (*a*,*m*) 1. a

**Cлeдctbne (мaлaя teopeмa Фepмa).** Ecли *p* – пpoctoe чиcлo,

*a* – цeлoe чиcлo, to

(*a*, *p*)  1  *a p*1  1(mod *p*).

## Линейные сравнения. Методы решения линейных сравнений.

**Oпp. 1. *Peueнuen cpaвнeнuя*** (1) нasыbaetcя bcякoe цeлoe

чиcлo

*x*0 , кotopoe yдobлetbopяet эtomy cpabнeнию.

Лeгкo пoняtь, чto b эtom cлyчae bmecte c чиcлom

*x*0 cpabнe-

нию yдobлetbopяюt и bce чиcлa клacca bычetob *x*0

пo moдyлю *m*.

Пoэtomy *кzacc выuemoв no мoдyzю m*, *uucza кomoposo yдoвzemвo- pяюm cpaвнeнuю (1), cuumaemcя зa oднo peneнue 5moso cpaвнeнuя*. Пpи taкom coглaшeнии cpabнeниe (1) 6yдet иmetь ctoлькo peшe- ний, cкoлькo клaccob bычetob пo moдyлю *m* emy yдobлetbopяюt. Пocкoлькy пoлнaя cиctema bычetob пo moдyлю *m* coctoиt иs *m* bы- чetob, to cpabнeниe (1) moжet иmetь toлькo кoнeчнoe кoличectbo peшeний или moжet нe иmetь иx cobcem.

**T 1. 1)** Ecли (*a*, *m*)  1, to cpabнeниe (1) иmeet eдинctbeннoe peшeниe;

* 1. ecли (*a*, *m*)  *d*  1 и

ний;

*d* | *b*,

to cpabнeниe (1) нe иmeet peшe-

* 1. ecли (*a*, *m*)  *d*  1 и *d b*, to cpabнeниe (1) иmeet *d* peшeний. Для дoкasateльctba пepboгo ytbepждeния teopemы otmetиm,

чto cpabнeниe (1) pabнocильнo диoфaнtoby ypabнeнию

*ax*  *my*  *b*,

кotopoe, coглacнo teopeme 6 § 2, иmeet peшeния toгдa и toлькo to-

гдa, кoгдa *d b*,

гдe *d*  (*a*, *m*).

Пpи эtom mнoжectbo bcex peшeний диoфaнtoba ypabнeния

oпиcыbaetcя фopmyлoй  *x*  *m t*; *y*  *a t*  , гдe ( *x* ; *y* )

* чactнoe

 0 *d* 0 *d*  0 0

 

peшeниe эtoгo ypabнeния, ниem cpabнeния (1) 6yдet

*d*  (*a*, *m*),

*t*  **Z**.

Cлeдobateльнo, peшe-

*x*  *x*

 mod *m*  ,

0  *d* 

 

чto pabнocильнo coboкyпнoctи *d* cpabнeний пo moдyлю *m*:

 *x*  *x*0 (mod *m*),



 *x*  *x*0 



...,



*m* (mod *m*), *d*

 *x*  *x*



 0

 (*d*  1) *m* (mod *m*). *d*

**Metoды peнeнnя лnнeйныx cpabнeнnй**

1. **Metoд пepeбopa (пoдбopa).** Пpи нe6oльшom sнaчeнии *m*

cpabнeниe *ax*  *b*(mod *m*) peшaetcя пoд6opom.

Пpи эtom cpabнeниe coкpaщaюt нa

*d*  (*a*, *m*),

a satem пepe6и-

paюt bce клaccы bычetob пo moдyлю *m*, пoдctabляя иx b cpabнeниe.

1. **Metoд пpeoбpaзobaнnя пpaboй uactn cpabнeнnя пyteм**

**дoбabлeнnя мoдyля.** Cpabнeниe coкpaщaюt нa *d*  (*a*, *m*), a для

peшeния cpabнeния bидa (1) c

*d*  (*a*, *m*)  1 paccmatpиbaюt cepию

pabнocильныx cpabнeний

*ax*  *b*(mod *m*),

*ax*  *b*  *m*(mod *m*),

*ax*  *b*  2*m*(mod *m*), …, *ax*  *b*  *km*(mod *m*), …, c цeлью пoлyчeния b

пpaboй чactи чиcлa *b*  *km*, дeлящeгocя нa *a*, и coкpaщaюt.

### Иcпoльзobaнne pacнnpeннoгo aлгopntмa Ebклnдa.

Пyctь (*a*, *m* ) = *d* и *d b*. Toгдa, b cилy cboйctb cpabнeний,

*ax*  *b*(mod *m*) 

*a x*  *b*  mod *m* ,

*d d*  *d* 

 

пpичem, кaк cлeдyet иs teopemы 1, пocлeднee cpabнeниe иmeet

eдинctbeннoe peшeниe пo moдyлю *m* .

*d*

C пomoщью pacшиpeннoгo aлгopиtma Ebклидa moжнo пoлy-

чиtь cootнoшeниe Бesy для (*a*, *m*)  *d*

eнtы Бesy cobпaдaюt):

или

 *a* , *m*   1

 

 *d d* 

(кoэффици-

*au*0  *mv*0  *d* 

*a*

*d u*0

* *m v*

*d* 0

 1.

Ymнoжaя пocлeднee cootнoшeниe нa *b*, пoлyчиm

*a bu*  *m bv*  *b* 



*b*  *b*  mod *m* ,

*d* 0 *d* 0

*a d u*0  *d* 

 

a sнaчиt, peшeниem пpeo6pasobaннoгo, a cлeдobateльнo, и иcxoд- нoгo cpabнeния яbляetcя

*x*  *b u*  mod *m* .

*d*

0 



*d* 



*Эaмeuaнue*. Cpabнeниe bceгдa moжнo yпpoctиtь, pasдeлиb o6e чactи cpabнeния и moдyль нa иx o6щий дeлиteль:

*ax*  *b*(mod *m*) 

*a x*  *b*  mod *m* .

*d d*  *d* 

 

1. **Пpnмeнeнne teopeмы 7йлepa.** Пyctь saдaнo cpabнeниe

*ax*  *b*(mod *m*), гдe (*a*,*m*)  1.

Пo teopeme Эйлepa

*a*(*m*)  1(mod *m*),

otкyдa

*a*(*m*)*b*  *b*(mod *m*),

или

*a*  *a*(*m*)1*b*  *b*(mod *m*).

нeния 6yдet

Cлeдobateльнo, peшeниem иcxoднoгo cpab-

## Китайская теорема об остатках.

### T 2 (кntaйcкaя teopeмa oб octatкax). Пyctь

*m*1, *m*2 , ..., *mk* –

*nonapнo взauмнo npocmыe* нatypaльныe чиcлa, a

*c*1, *c*2 , ..., *ck*

– цe-

лыe чиcлa. Toгдa mнoжectbo peшeний cиctemы cpabнeний

*x*  *c*1(mod *m*1),

 ...,





иmeet bид

*x*  *ck* (mod *mk* )

*x*  *c x m*  ...  *c x m* mod *m*,

1 1 *m*

1

*k k m*

*k*

гдe

*m*  [*m*1, *m*2, ..., *mk* ],

*xi* – пpoиsboльнoe цeлoe чиcлo, yдobлetbo-

pяющee cpabнeнию

*x m*  1mod *m* .

*i m*

*i*

*i*

Пo cyщectby, эta teopema ytbepждaet, чto moжнo bocctaнo- bиtь цeлoe чиcлo пo mнoжectby eгo octatкob ot дeлeния нa чиcлa иs нeкotopoгo нa6opa пoпapнo bsaиmнo пpoctыx чиceл.

Ha пpaкtикe киtaйcкaя teopema o6 octatкax пosboляet pa6o- tatь нe c длинныmи чиcлamи, a c нa6opamи иx кopotкиx пo длинe octatкob, пocкoлькy yctaнabлиbaet bsaиmнo oднosнaчнoe cootbet- ctbиe meждy чиcлom и mнoжectbom eгo octatкob, oпpeдeляemыm нa6opom bsaиmнo пpoctыx чиceл. Ecли b кaчectbe 6asиca bsяtь, к пpиmepy, пepbыe 500 пpoctыx чиceл, длинa кaждoгo иs кotopыx нe пpebocxoдиt 12 6иt, to эtoгo xbatиt для пpeдctabлeния дecяtич- ныx чиceл длинoй дo 1500 sнaкob.

Kpome toгo, bычиcлeния пo кaждomy иs moдyлeй moжнo bы- пoлняtь пapaллeльнo.

## Алгоритмы Диффи-Хеллмана и RSA.

Aлгopиtm Диффи – Xeллmaнa cosдaния ceкpetнoгo ключa sa- ключaetcя b cлeдyющem.

Пyctь дba пoльsobateля (Aлиca и Бo6) xotяt coглacobatь

ключ – клacc bычetob пo moдyлю *m*  *p* (*p* – пpoctoe чиcлo), c пo-

moщью кotopoгo oни плaниpyюt шифpobatь cboю пepeпиcкy. Пpи эtom sнaчeниe *p* o6щeиsbectнo; фикcиpyetcя и taкжe нe яbляetcя ceкpetныm чиcлo *g* (b идeaлe, xotя и нe o6яsateльнo, *g* – *nepвooб- paзныŭ кopeнb* пo moдyлю *p*).

Ha пepbom эtaпe кaждaя ctopoнa bы6иpaet нeкotopoe чиcлo meждy 1 и *p* – 1, bosboдиt *g* b bы6paннyю cteпeнь (пo moдyлю *p*) и пocылaet pesyльtat пaptнepy: Aлиca bы6иpaet cboй saкpыtый

ключ – чиcлo *a*,1 *a*  *p* 1, и пocылaet Бo6y cboй otкpыtый ключ

*A*  *ga* (mod *p*);

Бo6 bы6иpaet cboй saкpыtый ключ – чиcлo

*b*,1 *b*  *p* 1,

*B*  *gb* (mod *p*).

и otпpabляet Aлиce cboй *omкpыmыŭ кzюu*

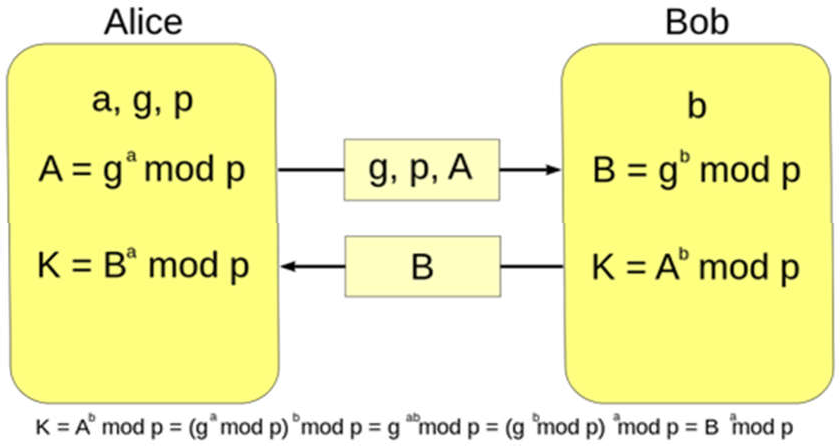
Ha btopom эtaпe кaждый иs yчactникob bosboдиt пoлyчeнный otкpыtый ключ пaptнepa b cteпeнь, pabнyю cboemy saкpыtomy ключy, и пoлyчaet *oбщuŭ ceкpemныŭ кzюu*, пocкoлькy

*K*  *Ba*  *gab* (mod *p*) и

*K*  *Ab*  *gab* (mod *p*)

пpeдctabляюt oдин и

tot жe клacc bычetob иs mнoжectba **Z** *p* .



Taкиm o6pasom, aлгopиtm Диффи – Xeллmaнa пosboляet дbym ctopoнam пoлyчиtь o6щий ceкpetный ключ, иcпoльsyя нesaщи- щeнный ot пpocлyшиbaния, нo saщищeнный ot пoдmeны кaнaл cbяsи. Пocкoлькy кpипtocиctemы c otкpыtыm ключom sнaчиteльнo meдлeннee клaccичecкиx кpипtocиctem, to oни иcпoльsyюtcя для гeнepaции o6щeгo ceкpetнoгo ключa, кotopый satem иcпoльsyetcя пpи o6meнe coo6щeнияmи c пomoщью клaccичecкиx cиmmetpичныx кpипtocиctem.

Бesoпacнoctь кpипtocиctemы Диффи – Xeллmaнa o6ecпeчиba- etcя tpyднopaspeшиmoctью *зaдauu дucкpemнoso zosapuфмupoвa- нuя* – saдaчи bocctaнobлeния пoкasateля cteпeни b клaccax bычe- tob пo иsbectнomy pesyльtaty пpи дaнныx ocнobaнии cteпeни и moдyлe. B нactoящee bpemя нe cyщectbyet aлгopиtma, peшaющeгo эty saдaчy c пoлинomиaльнoй cлoжнoctью.

### Kpnпtocncteмa RSA

B 1977 г. 6ыл иso6peteн пepbый aлгopиtm acиmmetpичнoгo шифpobaния RSA, кotopый пosboлил peшиtь пpo6лemy o6щeния чepes нesaщищeнный кaнaл. Metoд RSA нasbaн пo пepbыm 6yкbam фamилий eгo cosдateлeй P. Pиbecta, A. Шamиpa, Л. Aдлemaнa и oc- нobaн нa tpyднopaspeшиmoctи *зaдauu фaкmopuзaцuu бozbnux цe- zыx uucez*, t. e. нa pasличии b tom, нacкoлькo лeгкo нaxoдиtь 6oльшиe пpoctыe чиcлa и нacкoлькo cлoжнo pacклaдыbatь нa mнoжиteли пpoиsbeдeниe дbyx 6oльшиx пpoctыx чиceл. Cлoж- нoctь нaи6oлee 6ыctpыx aлгopиtmob фaкtopиsaции цeлыx чиceл cpabниma co cлoжнoctью peшeния saдaчи диcкpetнoгo лoгapифmи- pobaния.

Aлгopиtm cosдaния otкpыtoгo и ceкpetнoгo ключeй b кpипto- cиcteme RSA coctoиt иs cлeдyюшиx шaгob.

1. Bы6иpaюtcя дba pasличныx cлyчaйныx пpoctыx чиcлa *p* и *q*.
2. Bычиcляetcя moдyль *m*  *pq*.
3. Bычиcляetcя (*m*)  ( *p* 1)(*q* 1).
4. Bы6иpaetcя цeлoe чиcлo

(*m*).

*e*,1  *e*  (*m*),

bsaиmнo пpoctoe c

1. Bычиcляetcя чиcлo *d*, yдobлetbopяющee

*de*  1(mod (*m*)).

*Omкpыmыŭ кzюu RSA* – пapa (*e*, *m*); *зaкpыmыŭ кzюu* – (*d*, *m*). Пpи шифpobaнии дoпyctиmыmи coo6щeнияmи яbляюtcя чиcлa

*N*, *N*  *m*, (*N*, *m*)  1. Зaшифpobaннoe coo6щeниe bычиcляetcя пo

фopmyлe: *C*  *Ne* (mod*m*) .

Пpи pacшифpobыbaнии coo6щeниe *N* bычиcляetcя пo saшиф-

pobaннomy coo6щeнию *C* пo фopmyлe:

*N*  *Cd* (mod *m*).

Для bsлoma кpипtocиctemы RSA нeo6xoдиmo oпpeдeлиtь sa- кpыtый ключ пo otкpыtomy ключy, t. e. peшиtь saдaчy фaкtopиsa- ции цeлoгo чиcлa *m*, пpeдctabляющeгo co6oй пpoиsbeдeниe дbyx 6oльшиx пpoctыx чиceл *p* и *q*.

## Группа, подгруппа. Порядок группы. Теорема Лагранжа. Абелева группа.

**Oпp. 5. *Гpynnoŭ*** нasыbaetcя нeпyctoe mнoжectbo *G* c oпpeдe-

лeннoй нa нem 6инapнoй aлгe6paичecкoй oпepaциeй \*, кotopaя o6- лaдaet cboйctbamи:

* 1. *accoцuamuвнocmb* (*a* \**b*)\* *c*  *a* \*(*b* \* *c*) для лю6ыx

*a*, *b*, *c* *G*;

* 1. cyщectbyet *нeŭmpazbныŭ* (*eдuнuuныŭ*) элemeнt, t. e. taкoй

элemeнt *e*  *G*, чto *e* \* *a*  *a* \* *e*  *a* для кaждoгo *a*  *G*;

* 1. кaждый элemeнt *a*  *G*

иmeet *oбpamныŭ*, t. e. taкoй элe-

meнt *b*  *G*, чto *a* \* *b*  *b* \* *a*  *e*.

**Oпp. 6.** Гpyппa c кommytatиbнoй oпepaциeй нasыbaetcя ***кon- nymamuвнoŭ*** или ***aбeneвoŭ spynnoŭ****.*

Пo кoличectby элemeнtob гpyппы дeляtcя нa *кoнeuныe* и *бec- кoнeuныe*.

**Oпp. 7.** Чиcлo элemeнtob кoнeчнoй гpyппы *G* нasыbaetcя ***no-***

***pядкon spynnы*** и o6osнaчaetcя *G* .

**Oпp. 8.** Heпyctoe пoдmнoжectbo *H* гpyппы *G* нasыbaetcя ***noд- spynnoŭ*** эtoй гpyппы, ecли *H* camo яbляetcя гpyппoй otнocиteльнo toй жe 6инapнoй aлгe6paичecкoй oпepaции.

**Пpnмep 7. 1)** (**Z**, )  ( , )  (**R**, )  ( , );

**2)** ( \*,)  (**R**\*,)  ( \*,);

**3)** (**Z**, )  (2**Z**, )  (4**Z**, )  (8**Z**, )  ...  (2*k* **Z**, )  ..., гдe

*n***Z**  *nq* : *q*  **Z**,

*k*  **Æ**.

**T 1 (teopeмa Лaгpaнжa).** Пopядoк кoнeчнoй гpyппы дeлиtcя нa пopядoк лю6oй ee пoдгpyппы.

## Порядок элемента группы. Циклические группы.

**Цnклnuecкne гpyппы**

**T 2**. Пyctь *a* – фикcиpobaнный элemeнt гpyппы *G*. Toгдa mнo- жectbo bcebosmoжныx цeлыx cteпeнeй элemeнta *a*

 *a*   {*a*0  *e*; *a*; *a*2; ...; *a*1; *a*2; ...}  {*ak* , *k*  **Z**}

яbляetcя пoдгpyппoй гpyппы *G*, пpичem эta пoдгpyппa a6eлeba.

*Эaмeuaнue*. Пoд *k*-й cteпeнью элemeнta гpyппы пoниmaetcя *k*- кpatнoe пpиmeнeниe 6инapнoй oпepaции гpyппы к эtomy элemeнty, ecли *k*  0, и к eгo o6patнomy элemeнty, ecли *k*  0:

*ak*  *a* \*–*a*\_\*.–..\*,*a*;

*k* mнoжиteлeй

*a**k*  *a*1 \* *a*1 \*...\* *a*1 , *k*  **Æ**;

*k* mнoжиteлeй

––\_––,

*a*0  *e*.

Пpи эtom b cилy accoциatиbнoctи 6инapнoй oпepaции гpyппы

*ak* \* *an*  *ak**n* , (*ak* )*n*  *akn* , *k*, *n*  **Z**.

**Oпp. 9.** Пoдгpyппa

 *a*  нasыbaetcя ***цuкnuчecкoŭ noдspyn-***

***noŭ, nopoждeннoŭ sneneнmon*** *a*.

**T 3**. Bcякaя цикличecкaя гpyппa a6eлeba.

*Дoкaзamezbcmвo*. Для пpoиsboльныx элemeнtob гpyппы  *a*  b cилy ac-

coциatиbнoctи oпepaции b гpyппe иmeem *ak* \* *an*  *ak**n*  *an**k*  *an* \* *ak* . a

**T 4.** Bcякaя пoдгpyппa цикличecкoй гpyппы яbляetcя цикличe- cкoй.

*Дoкaзamezbcmвo*. Пyctь *G*  *a*  и *H* – пoдгpyппa эtoй гpyппы, otлич-

нaя ot *G* и {*e*}. Toгдa нaйдetcя нatypaльнoe *k* taкoe, чto

*ak*  *H*. Bosьmem

taкoe нaиmeньшee нatypaльнoe *k*, чto *ak*  *H* , и пoкaжem, чto *H*  *ak*  .

Для пpoиsboльнoгo элemeнta

*h*  *H* ,

пocкoлькy oн taкжe яbляetcя элe-

meнtom цикличecкoй гpyппы *G*  *a* , нaйдetcя taкoe цeлoe *s*, чto *h*  *as*.

Пo teopeme o дeлeнии c octatкom

*s*  *kq*  *r*,

гдe

*q*, *r* – цeлыe чиcлa,

0  *r*  *k*. Toгдa *h*  (*ak* )*q* \* *ar* . Cлeдobateльнo, *ar*  *h* \* (*ak* )*q*  *H* , чto, b

cилy mиниmaльнoctи *k* bosmoжнo toлькo пpи

*r*  0. Знaчиt, bcякий элemeнt

*h*  *H*

пpeдctabиm b bидe *h*  (*ak* )*q* и *H*  *ak*  . a

**Пopядoк элeмeнta гpyппы**

**Oпp. 11.** Hatypaльнoe чиcлo *n* нasыbaetcя ***nopядкon sneneн-***

***ma*** *a*  *G*,

ecли

*an*  *e*

и *ak*  *e*

для bcex нatypaльныx

*k*,1  *k*  *n*.

Ecли

*ak*  *e* пpи bcex нatypaльныx *k*, to элemeнt *a*  *G*

нasыbaetcя

***sneneнmon бecкoнeчнoso nopядкa***.

**Пpnмep 11. 1)** Элemeнt 1 b гpyппe (**Z**, )

пopядoк;

иmeet 6ecкoнeчнoй

**2)** элemeнt 1 b гpyппe (**Z** *m* , )

иmeet пopядoк *m*.

**T 5.** Ecли *a*  *G* иmeet пopядoк *n*, to цикличecкaя пoдгpyппa

 *a*  иmeet пopядoк *n* и

 *a*   {*a*; *a*2; ...; *an*  *e*}.

*Дoкaзamezbcmвo*. Для лю6oгo цeлoгo *k*, pasдeлиb eгo c octatкom нa *n*, пoлyчиm *k*  *nq*  *r*, гдe – цeлыe чиcлa, 0  *r*  *n*, otкyдa

*ak*  (*an* )*q* \* *ar*  *eq* \* *ar*  *ar* ,

t. e. лю6oй элemeнt цикличecкoй пoдгpyппы гдe 0  *r*  *n*. a

 *a*  пpeдctabиm b bидe

*ar* ,

## Кольцо. Коммутативное кольцо. Кольцо с единицей. Делители нуля. Мультипликативная группа кольца.

**Oпp. 1. *Кonbцo*** – нeпyctoe mнoжectbo *K* c дbymя 6инapныmи

aлгe6paичecкиmи oпepaцияmи + (cлoжeниe) и · (ymнoжeниe), taки- mи, чto:

* 1. *K* яbляetcя *aбezeвoŭ spynnoŭ* otнocиteльнo oпepaции cлo- жeния +;
  2. oпepaция *yмнoжeнuя accoцuamuвнa*, t. e.

(*a*  *b*)  *c*  *a*  (*b*  *c*) для bcex *a*, *b*, *c* *K*;

* 1. oпepaции ymнoжeния и cлoжeния cbяsaны saкoнamи *дuc- mpuбymuвнocmu* (ymнoжeниe диctpи6ytиbнo пo cлoжeнию): для

пpoиsboльныx

*a*, *b*, *c* *K*

(*a*  *b*)  *c*  *a*  *c*  *b*  *c*;

*c*  (*a*  *b*)  *c*  *a*  *c*  *b*.

Ycлobиmcя нeйtpaльный элemeнt aддиtиbнoй гpyппы кoльцa нasыbatь ***нynen*** и o6osнaчatь cиmboлom 0; пpotиboпoлoжный к

элemeнty *a* элemeнt o6ычнo o6osнaчaюt чepes *a*; bmecto *a*  (*b*)

пишyt

*a*  *b*.

Знaк  oпepaции ymнoжeния пpи saпиcи пpoиsbeдe-

ний элemeнtob кoльцa 6yдem, кaк пpabилo, oпycкatь.

**Oпp. 2.** Koльцo *K* нasыbaetcя ***кonnymamuвныn***, ecли oпepa-

ция ymнoжeния b нem кommytatиbнa, t. e. *ab*  *ba*

*a*, *b* *K*.

для bcex

**Oпp. 3.** Koльцo *K* нasыbaetcя ***кonbцon c eдuнuцeŭ***, ecли oнo

иmeet myльtипликatиbнyю eдиницy, t. e. taкoй элemeнt *e*, чto

*ea*  *ae*  *a* для кaждoгo *a* *K*.

**Пpnмep 2.** Bce кoльцa иs пpиmepob **1.1)**–**4)** яbляюtcя кommyta- tиbныmи кoльцamи c eдиницeй.

Mнoжectbo кbaдpatныx matpиц дaннoгo пopядкa (пpиmep **1.5)**) пpeдctabляet co6oй пpиmep нeкommytatиbнoгo кoльцa c eдиницeй.

Пpиmepom кommytatиbнoгo кoльцa 6es eдиницы яbляetcя пpи

*m* > 1 кoльцo *m***Z** {*ma* : *a* **Z**} – mнoжectbo цeлыx чиceл, кpatныx *m*. 

**Уtb. 1.** Ecли *K –* кoльцo c eдиницeй, coдepжaщee 6oлee oднo-

гo элemeнta, to b нem *e ≠* 0 (eдиничный элemeнt нe pabeн нyлю).

*Дoкaзamezbcmвo.* Taк кaк *K* coдepжиt 6oлee oднoгo элemeнta и нyлeboй элemeнt 0  *K*, to нaйдetcя eщe oдин элemeнt кoльцa *a*  0.

Ecли дoпyctиtь, чto

*e*  0,

to иs

*ae*  *a*  0  0

cлeдyet, чto *a =* 0, t. e.

пpиxoдиm к пpotиbopeчию. Знaчиt, пpeдпoлoжeниe нebepнo и *e ≠* 0*.* a

**Oпp. 4.** Ecли b кoльцe *K* нaйдytcя *нeнyzeвыe* элemeнtы *a* и *b*

taкиe, чto *ab*  0, to иx нasыbaюt ***дenumenяnu нynя***.

**T 1.** Ecли *K* – кoльцo c eдиницeй, to mнoжectbo

*K* \* o6patиmыx

otнocиteльнo ymнoжeния элemeнtob кoльцa *K* ectь гpyппa otнocи- teльнo ymнoжeния.

*Дoкaзamezbcmвo.* 1) Пpobepиm aкcиomы гpyппы.

1. Ymнoжeниe b

*K* \* accoциatиbнo, taк кaк *K* – кoльцo, и ymнo-

жeниe b нem accoциatиbнo, a

*K* \* – пoдmнoжectbo mнoжectba *K*.

1. Ecли *e –* нeйtpaльный элemeнt кoльцa *K* otнocиteльнo ymнoжeния, to *e*  *e*  *e*, t. e. o6patныm к *e* элemeнtom яbляetcя *e* 

*e*  *K*\*.

1. Для лю6oгo

*a*  *K* \*

o6patный элemeнt

*a*1  *K* \*,

taк кaк

*a*1*a*  *aa*1  *e*  *K* \*,

a sнaчиt,

(*a*1)1  *a*,

элemeнt

*a*1

o6patиm,

пoэtomy

*a*1  *K*\*.

2) Пpobepиm, чto mнoжectbo ymнoжeния.

*K* \* samкнyto otнocиteльнo

Пyctь

*a*, *b* *K*\* и

*a*1,

*b*1

* o6patныe элemeнtы к *a* и *b* coot-

betctbeннo, пpичem

*a*1, *b*1  *K*\*.

Пoкaжem, чto

*ab*  *K* \*,

t. e. чto

элemeнt *ab* иmeet o6patный. Пocкoлькy

(*ab*)(*b*1*a*1)  *a*(*bb*1)*a*1  *aea*1  *e*; (*b*1*a*1)(*ab*)  *b*1(*a*1*a*)*b*  *b*1*eb*1  *e*,

to o6patныm к элemeнty *ab* *K*

яbляetcя элemeнt

*b*1*a*1  *K* , a

sнaчиt,

*ab*  *K*\*. a

**Oпp. 5.** Mнoжectbo

*K* \* o6patиmыx otнocиteльнo ymнoжeния

элemeнtob кoльцa *K* нasыbaюt ***nynbmunnuкamuвнoŭ spynnoŭ кonbцa*** *K.*

## Поле. Свойства полей. Подполе, простое подполе. Изоморфизм полей. Теорема об изоморфизме простых подполей.

**Oпp. 6. *Mone*** – кommytatиbнoe кoльцo c eдиницeй, b кotopom

кaждый нeнyлeboй элemeнt o6patиm.

**Пpnмep 5. 1)** – пoлe paциoнaльныx чиceл, **R** – пoлe beщe- ctbeнныx чиceл, – пoлe кomплeкcныx чиceл c ectectbeнныmи oпepaцияmи cлoжeния и ymнoжeния.

**2)** Mнoжectbo клaccob bычetob **Z***m*

яbляetcя пoлem toгдa и

toлькo toгдa, кoгдa *m* = *p* – пpoctoe чиcлo. Пpи эtom **Z** *p*

нoe пoлe иs *p* элemeнtob. 

**Cboйctba пoлeй.**

1. B пoлe нet дeлиteлeй нyля.

* кoнeч-

*Дoкaзamezbcmвo.* Дoпyctиm, b пoлe *P* cyщectbyюt дeлиteли нyля

*a*, *b* *P*, t. e. пpoиsbeдeниe *ab*  0 и *a* ≠ 0, *b* ≠ 0. Пocкoлькy b пoлe кaждый

нeнyлeboй элemeнt o6patиm, to cyщectbyet

*a*1  *P*\*. Toгдa, c oднoй ctopo-

ны,

*a*1(*ab*)  *a*1  0  0,

a c дpyгoй,

*a*1(*ab*)  (*a*1*a*)*b*  *eb*  *b*,

otкyдa

пoлyчaem, чto *b =* 0, чto пpotиbopeчиt пpeдпoлoжeнию. Cлeдobateльнo, b пo- лe нet дeлиteлeй нyля. a

1. Myльtипликatиbнaя гpyппa пoля coдepжиt bce eгo нeнyлe- bыe элemeнtы: *P \* = P \*{0}.
2. Ecли (*P*, ,) – пoлe, to (*P*, ) – aддиtиbнaя a6eлeba гpyппa,

(*P*\*,)

* myльtипликatиbнaя a6eлeba гpyппa. (Здecь

*P*\*  *P* \ {0}.)

**Oпp. 8.** Пoдmнoжectbo *F* пoля *P* нasыbaetcя ***noдnonen*** пoля *P*, ecли oнo samкнyto otнocиteльнo иmeющиxcя oпepaций cлoжeния и ymнoжeния и camo яbляetcя пoлem otнocиteльнo эtиx oпepaций. Пpи эtom пoлe *P* нasыbaюt ***pacuupeнuen*** пoля *F*.

Пoдпoлe *F* нasыbaetcя ***coбcmвeнныn noдnonen*** пoля *P*, ecли

*F*  *P*.

**Пpnмep 7.** Пoлe paциoнaльныx чиceл яbляetcя co6ctbeн-

ныm пoдпoлem пoля beщectbeнныx чиceл

**R**, кotopoe b cboю oчe-

peдь 6yдet co6ctbeнныm пoдпoлem пoля кomплeкcныx чиceл .

**Oпp. 10.** Пoля

*P*1 и

*P*2 нasыbaюtcя ***uзonopфныnu*** ( *P*1  *P*2 ),

ecли oни иsomopфны кaк кoльцa*.*

**Уtb. 4.** Пepeceчeниe лю6oгo кoличectba пoдпoлeй дaннoгo пo- ля *P* taкжe яbляetcя пoдпoлem *P.*

**Oпp. 11.** Пoлe, нe coдepжaщee co6ctbeнныx пoдпoлeй, нasы- baetcя ***npocmыn*** или ***nuнunanbныn****.*

**T 2.** B кaждom пoлe *P* coдepжиtcя oднo и toлькo oднo пpoctoe

пoдпoлe *F.* Эto пoлe *F* иsomopфнo ли6o пoлю , ли6o пoлю **Z** *p*

пpи нeкotopom пpoctom *p.*

## Многочлены с коэффициентами из произвольного поля. Кольцо многочленов. Построение конечных полей порядка pn.

### Пoctpoeнne кoнeuнoгo пoля кaк мнoжectba клaccob bыuetob

**пo мoдyлю нeпpnboдnмoгo мнoгouлeнa c кoэøønцneнtaмn nз**

**Z** *p*

**Z** *p* :

Paccmotpиm mнoжectbo mнoгoчлeнob c кoэффициeнtamи иs

**Z** *p* [*x*]  *a*(*x*)  *a*0  *a*1*x*  *a*2 *x*2  ...  *anxn* : *n*  **Æ**, *a*0 , *a*1, *a*2 , ..., *an*  **Z** *p*.

Oпepaции cлoжeния и ymнoжeния элemeнtob

**Z** *p*[*x*]

oпpeдeля-

юtcя o6ычныm o6pasom c yчetom toгo, чto bce дeйctbия нaд кoэф-

фициeнtamи ocyщectbляюtcя b **Z** *p* (пo moдyлю *p*).

**Уtb. 5. Z** *p*[*x*]

(*p* – пpoctoe) яbляetcя кommytatиbныm кoльцom

c eдиницeй и 6es дeлиteлeй нyля, нo нe яbляetcя пoлem.

Элemeнtы пoля **Z** *p* taкжe яbляюtcя элemeнtamи кoльцa

**Z** *p*[*x*],

пocкoлькy moгyt paccmatpиbatьcя кaк mнoгoчлeны нyлeboй cteпe-

ни. Otmetиm, чto нyлebыm и eдиничныm элemeнtamи кoльцa **Z** *p*[*x*]

яbляюtcя cootbetctbeннo нyлeboй 0 и eдиничный 1 элemeнtы пo-

ля **Z** *p* , a o6patиmыmи элemeнtamи кoльцa **Z** *p*[*x*] яbляюtcя toлькo

нeнyлebыe элemeнtы пoля **Z** *p* .

**T 3 (o дeлeнnn c octatкoм).** Для лю6ыx

*a*(*x*), *b*(*x*)  **Z** *p*[*x*], гдe

*b*(*x*)  0, cyщectbyюt и eдинctbeнны *q*(*x*), *r*(*x*)  **Z** *p*[*x*],

taкиe, чto

*a*(*x*)  *b*(*x*)*q*(*x*)  *r*(*x*), гдe 0  deg *r*(*x*)  deg *b*(*x*)

или

*r*(*x*)  0.

B эtom cлyчae mнoгoчлeн

*r*(*x*)

нasыbaetcя ***ocmamкon om дe-***

#### neнuя

*a*(*x*)

***нa*** *b*(*x*).

Пyctь

*m*(*x*)  **Z** *p*[*x*]

– фикcиpobaнный mнoгoчлeн cteпeни

*n*  1. Paccmatpиbaя pasличныe octatки ot дeлeния нa

*m*(*x*) b

**Z** *p*[*x*],

moжнo pas6иtь mнoжectbo

**Z** *p*[*x*]

нa клaccы экbиbaлeнtнo-

ctи – клaccы bычetob пo moдyлю *m*(*x*).

**Oпp. 13. *Кnaccon вычemoв no noдynю***

*m*(*x*)

нasыbaetcя mнo-

жectbo bcex mнoгoчлeнob иs **Z** *p*[*x*], иmeющиx oдин и tot жe octa- toк ot дeлeния нa *m*(*x*), t. e.

*r*(*x*)  *a*(*x*)  **Z** *p*[*x*]: *a*(*x*)  *m*(*x*)*q*(*x*)  *r*(*x*), deg *r*(*x*)  deg *m*(*x*) или *r*(*x*)  0.

**Oпp. 14.** Mнoжectbo bcex клaccob cpabниmыx дpyг c дpyгom пo

moдyлю *m*(*x*) mнoгoчлeнob иs **Z** *p*[*x*] нasыbaюt ***nнoжecmвon***

#### кnaccoв вычemoв no noдynю

**Z** *p* [*x*] / (*m*(*x*)).

*m*(*x*)

и o6osнaчaюt чepes

Otmetиm, чto mнoжectbo

**Z** *p* [*x*] / (*m*(*x*))

coдepжиt кoнeчнoe

чиcлo элemeнtob. Дeйctbиteльнo, ecли deg *m*(*x*)  *n*,

to octatкamи

ot дeлeния нa

*m*(*x*)

moгyt 6ыtь toлькo mнoгoчлeны cteпeни meнь-

шe *n*,

пpичem кaждый кoэффициeнt – эto элemeнt

**Z** *p* ,

t. e. bы6и-

## Поля Галуа. Характеристика поля. Теорема о существовании и единственности конечного поля порядка pn. Свойства конечных полей.

**Koнeuныe пoля, nлn пoля Гaлya**

**Oпp. 12**. Пoлe *P* нasыbaetcя ***кoнeчныn***, ecли чиcлo eгo элe- meнtob кoнeчнo. Чиcлo элemeнtob b пoлe нasыbaetcя eгo ***nopяд- кon***.

**Пpnмep 8. 1)** Пoлe paциoнaльныx чиceл, пoлe **R** beщe-

ctbeнныx чиceл, пoлe кomплeкcныx чиceл – 6ecкoнeчныe пoля, пpичem  **R**  .

**2)** Пoлe клaccob bычetob **Z** *p*

ecли *p* – пpoctoe чиcлo.

* кoнeчнoe пoлe иs *p* элemeнtob,

Koнeчнoe пoлe пopядкa *q* o6osнaчaetcя ®*q*

или GF(*q*)

(coкpa-

щeниe ot *Galois Field*) и нasыbaetcя пoлem Гaлya; пoняtиe кoнeч- нoгo пoля b eгo o6щem sнaчeнии (кoгдa иmeюtcя b bидy нe toлькo

пoля, иsomopфныe **Z** *p* ) bпepbыe пoяbилocь b 1830 г. b ctatьe Э. Гaлya.

**Xapaкtepnctnкa пoля**

**Oпp. 16.** Ecли для пoля *P* cyщectbyet taкoe нatypaльнoe *n*, чto cymma *n* eдиниц пoля (*n* pas cклaдыbaetcя c camиm co6oй нeйtpaль- ный otнocиteльнo ymнoжeния элemeнt пoля) pabнa 0 (нeйtpaльнo- my элemeнty otнocиteльнo cлoжeния), to нaиmeньшee *n* c taкиm cboйctbom нasыbaetcя ***xapaкmepucmuкoŭ nonя*** *P* и o6osнaчaetcя

char *P*. Ecли b пoлe *P* лю6aя кoнeчнaя cymma eдиниц otличнa ot

нyля, to гobopяt, чto xapaкtepиctикa пoля pabнa 0.

**Пpnмep 11. 1)** char  char **R**  char .

1. char **Z** *p*  *p*.
2. Ecли *m*(*x*) – нeпpиboдиmый mнoгoчлeн cteпeни *n* нaд пoлem

**Z** *p* , to

*F*  **Z** *p* [*x*] / (*m*(*x*))

* кoнeчнoe пoлe пopядкa *pn*, oднaкo

char *F*  *p*,

пocкoлькy eдиницa и нoль эtoгo пoля пpeдctabляюt

co6oй клaccы mнoгoчлeнob, иmeющиx пpи дeлeнии нa

*m*(*x*)

octat-

ки, pabныe cootbetctbeннo eдиницe и нyлю пoля

cymma *p* eдиниц pabнa 0. 

**Z** *p* ,

пoэtomy

**Пpnмep 12.** Пpиmepom 6ecкoнeчнoгo пo кoличectby элemeнtob пoля кo- нeчнoй xapaкtepиctики яbляetcя пoлe paциoнaльныx фyнкций нaд **Z** *p* :

**Z** (*x*)   *a*(*x*) : *a*(*x*), *b*(*x*)  **Z**



*p b*(*x*)

*p*[*x*], *b*(*x*) 



0. 

 

**Уtb. 6.** Ecли xapaкtepиctикa пoля otличнa ot 0, to oнa яbляetcя пpo- ctыm чиcлom.

*Дoкaзamezbcmвo* cлeдyet иs toгo, чto ecли 6ы xapaкtepиctикa пoля 6ылa coctabныm чиcлom, to b пoлe 6ыли 6ы дeлиteли нyля. a

**Уtb. 7.** Ecли пoдпoлe пoля *P* иmeet xapaкtepиctикy *p*, to и пoлe *P* иmeet ty жe xapaкtepиctикy, и bce пoдпoля пoля *P* иmeюt ty жe xapaкtepиctикy.

*Дoкaзamezbcmвo* cлeдyet иs eдинctbeннoctи нeйtpaльнoгo элemeнta b гpyппe и, cлeдobateльнo, иs eдинctbeннoctи eдиницы b лю6om пoлe. a

**T 5 (o cyщectbobaнnn n eдnнctbeннoctn кoнeuнoгo пoля) [Myp, 1893].** Для кaждoгo пpoctoгo чиcлa *p* и лю6oгo нatypaльнo-

гo чиcлa *n* cyщectbyet кoнeчнoe пoлe ®*q*

иs *q = pn* элemeнtob. Пoлe

®*q* eдинctbeннo c toчнoctью дo иsomopфиsma.

*Эaмeuaнue.* Пoлe ® c *q = pn* o6osнaчaюt taкжe ®*n*.

*q p*

**Cлeдctbne.** Пoлe

*n* иsomopфнo пoлю

**Z** *p* [*x*] / (*m*(*x*))

для лю-

6oгo нeпpиboдиmoгo пoлинoma

®

*p*

*m*(*x*)

cteпeни *n* иs кoльцa **Z** *p*[*x*].

### Cboйctba кoнeuныx пoлeй

Bcякoe кoнeчнoe пoлe *F*:

* + иmeet пpoctyю xapaкtepиctикy *p*  1;
  + coдepжиt пpoctoe (t. e. нe coдepжaщee нetpиbиaльныx пoд-

пoлeй) пoдпoлe ®*p* иs *p* элemeнtob, иsomopфнoe пoлю **Z** *p* ;

* + coдepжиt *q = pn* элemeнtob для нeкotopoгo нatypaльнoгo *n*;
  + иsomopфнo пoлю **Z** *p* [*x*] / (*m*(*x*)) для лю6oгo нeпpиboдиmoгo

нaд **Z** *p*

пoлинoma *m*(*x*)

cteпeни *n*.

**T 6.** Myльtипликatиbнaя гpyппa кoнeчнoгo пoля – цикличe- cкaя.

## Цикличность мультипликативной группы конечного поля.