Number Theory

content

1 Divisibility Theory **3**

1.1 Divisibility 3

1.2 Greatest Common Divisor(GCD) 3

1.3 Euclidean Alorithm 4

1.4 Least Common Mutiple 5

1.5 Prime Number 5

1.6 Fundamental Theorem Arithmetic 5

1.7 Exercise 6

2 Congruence **8**

2.1 The Difinition and Property of Congruence 8

2.2 Euler's Totient Function 9

2.2.1 Euler Theorem 10

2.2.2 Fermat's Little Theorem 10

2.3 Exercise: 10

3 Congruence Equation **11**

3.1 Residue System 11

3.1.1 Complete Residue System 11

3.1.2 Reduced Residue System 11

3.2 Linear Congruence Equation 11

3.2.1 Linear Congruence Equation 11

3.2.2 Linear Congruence Equation Set 12

3.2.3 Chinese Remainder Theorem 13

3.3 Polynomial Congruence Equation 13
3.4 Wilson Theorem 13
3.5 Exercise: 14

4 Quadratic Residue **15**
4.1 Difinition and Property of Quadratic Residue 15
4.2 Legendre Symbol 15
4.2.1 Quadratic Reciprocity Law 16
4.3 Jacobi Symbol 16
4.4 Exercise: 17

5 Discrete Logarithm **17**
5.1 Index and Primitive Root 17
5.2 Existence of Primitive Root 18
5.3 Discrete Logarithm 18

1 Divisibility Theory

1.1 Divisibility

$\forall$a,b$\in$ $\mathbb{Z}$,b$\neq$0,if there is a integer q let:

$$a = qb$$

then it is called that b can be divided by a or b divides b,marked as b|a,and b is a divisor of ,a is a mutiple of b.Otherwise marked as b$\nmid$a.

Specially,if a$\neq$0,and a is an integer,then a|0.

Theorem: suppose a,b,c$\in\mathbb{Z}$

(1)if b|a and a|b,then a=$\pm$b

(2)if a|b,and b|c,then a|c

(3)if c|a and c|b,then c|ua+vb,u,v$\in\mathbb{Z}$

(4)if c|$a_1\cdots$c|a_k,then $\forall u_1\cdots u_k$$\in\mathbb{Z}$,there is c|$(u_1a_1\cdots u_ka_k)$

(5)if m$\neq$0 and a|b $\Leftrightarrow$ ma|mb

(6)if a=qb+r and b|a $\Leftrightarrow$ b|r

Prove:

(1)(2)(4)(5)(6)skip

(3) suppose a=qc,b=pc,then ua+vb=uqc+vpc,obviously

1.2 Greatest Common Divisor(GCD)

if $\exists$q,a=qr_1,b=qr_2,r_1,$r_2$$\in\mathbb{Z}$,then q is called a common divisor of a and b,$\mathcal{D}$(a_1,$\cdots$,a_k)is a set of all common divisors of a_1,$\cdots$,a_k

if $\exists$d$\in\mathcal{D}$(a,b) and $\forall d_i$$\in\mathcal{D}$(a,b),$d_i$|d,then d is the great common divisor of a and b,marked as d=(a,b) or d=gcd(a,b)

Theorem: a,b$\in\mathbb{Z}$

(1)(a,b)=(a,-b)=(-a,b)=(-a,-b)=(|a|,|b|)

(2)(0,a)=|a|

(3)if a_i|a_j,j=1$\cdots$k,(a_1,$\cdots$,a_i,$\cdots$,a_k)=|a_i|

Prove:
(1)(2)(3)skip

1.3 Euclidean Alorithm

When a and b is large,to figure out their gcd directly is difficult,Euclidean Alorithml can be used to figure out their gcd

Suppose a,b∈$\mathbb{Z}$,let r_0=a,r_1=b,then:

$$\begin{aligned}
r_0 &= q_1r_1 + r_2 \quad 0 \le r_2 < r_1 \\
r_1 &= q_2r_2 + r_3 \quad 0 \le r_3 < r_2 \\
&\vdots \\
r_{k-2} &= q_{k-1}r_{k-1} + r_k \quad 0 \le r_k < r_{k-1} \\
r_{k-1} &= q_kr_k
\end{aligned}$$

Now r_k=(a,b)

Prove:

if $\exists r_i$,r_{i-1} ,$r_i|r_{i-1}$,then r_{i-1}=q_ir_i ,otherwise,because b=r_1>r_2>$\cdots$>r_k>0 ,b is limited,so that r_i≥r_{i-1}-1 ,and b-i+1≥r_i≥0 , when b-i+1=1 , then i=b , now r_i=1 , so that r_{i-1}=q_i , therefore we can always get the equation r_{k-1}=q_kr_k , now

$$\begin{aligned}
&r_{k-2} = q_{k-1}r_{k-1} + r_k = q_{k-1}q_kr_k + r_k \\
&r_{k-3} = q_{k-2}r_{k-2} + r_{k-1} = q_{k-2}(q_{k-1}q_kr_k + r_k) + q_kr_k = r_k(q_{k-2}q_{k-1}q_k + q_{k-2} + q_k) \\
&\quad\vdots \\
&\quad b = r_1 = X_1r_k \\
&\quad a = r_0 = X_2r_k
\end{aligned}$$

How to confirm r_k is greatest?

Construct contradiction

Corollary:

∃u,v∈$\mathbb{Z}$, ∀a,b∈$\mathbb{Z}$, let

$$(a, b) = ua + vb$$

1.4 Least Common Mutiple

if ∃c , q_1 , q_2∈ℤ , for a and b , c=q_1a=q_2b ,then c is a common mutiple of a and b , suppose $\mathcal{L}(a_1 \cdots a_k)$ is a set of all common mutiples of $a_1 \cdots a_k$

if ∃l∈$\mathcal{L}$(a,b) and $\forall l_i \in \mathcal{L}$(a,b) , l|$l_i$, then l is called least common mutiple , marked as [a,b] or lcm(a,b)

1.5 Prime Number

if $\mathcal{D}$(p)={1,p},p is called prime number

if (a,b)=1 , it is called a and b are relatively prime and $exists$u,v∈ℤ , let au+bv=1

Lemma:

(a,b)=1 ⇔ au+bv=1 , u,v∈ℤ

(a,p)=1,a=1⋯2p-1 , p is a prime

1.6 Fundamental Theorem Arithmetic

∀N∈ℤ and N>1,∃$P_1 \cdots P_k$, $a_1 \cdots a_k$∈ℤ , ∀P_i>1 , a_i>1 , let

$$N = \prod_{i=1}^{k} P_i^{a_i}$$

suppose

$$N_1 = \prod_{i=1}^{k_1} P_{1i}^{a_{1i}}$$

$$N_2 = \prod_{i=1}^{k_2} P_{2i}^{a_{2i}}$$

let

$$S_1 = \{P_{11}, \cdots, P_{1k_1}\}$$

$$S_2 = \{P_{21}, \cdots, P_{2k_2}\}$$

if

$$S_1 \bigcup S2 = \emptyset$$

then

$$(N_1, N_2) = 1$$

$$[N_1, N_2] = N_1 N_2$$

if

$$S_1 \bigcup S2 = S$$

$$S = \{P_j, \cdots, P_{j+l}\}$$

then

$$(N_1, N_2) = D = \prod_{i=j}^{j+l} P_i^{a_i} \qquad a_i = min\{a_{1j}, a_{2j}\}$$

and

$$(\frac{N_1}{D}, \frac{N_2}{D}) = 1$$

therefore

$$[\frac{N_1}{D}, \frac{N_2}{D}] = \frac{N_1 N_2}{D^2}$$

suppose

$$\begin{aligned} a, b \in \mathbb{Z}, m \neq 0, (a, b) = d \\ a = q_1 d, b = q_2 d \\ ma = q_1 dm, mb = q_2 dm \\ (ma, mb) = dm = (a, b) \times m \end{aligned}$$

therefore

$$[D \times \frac{N_1}{D}, D \times \frac{N_2}{D}] = D \times \frac{N_1 N_2}{D^2}$$

$$[N_1, N_2] = \frac{N_1 N_2}{D} = \frac{N_1 N_2}{(N_1, N_2)}$$

1.7 Exercise

(1) if $(a, b) = 1 \Rightarrow (a^n, b^n) = 1$

(2) if $a^n \mid b^n \Rightarrow a \mid b$

(3) if $a \mid n$, $b \mid n \Rightarrow [a, b] \mid n$

(4) if $a \mid n$ and $b \mid n$, whether $\exists u, v$, let $ua + vb = n$

(5) if $2^n - 1$ is a prime $\Rightarrow$ n is a prime

(6) if $\exists\sqrt{m}, \sqrt{n} \in \mathbb{Z}, \forall k \in \{k = x \mid x\ is\ a\ odd\ number\} \Rightarrow k = m - n$

(7)$\frac{n^5}{5} + \frac{n^3}{3} + \frac{7n}{15} \in \mathbb{Z}$

(8) $\forall x, y \ \Rightarrow \ 8 \nmid x^2 - y^2 - 2$

(9) if $n = c_k \cdot 10^k + \cdots + c_1 \cdot 10 + c_0$ and $11 \mid n \Leftrightarrow 11 \mid \ \sum_{i=0}^{k} (-1)^i c_{k-i}$

(10) if $m, n \in \mathbb{Z}$ no matter how to choose the $+, -$, $\sum_{i=0}^{n}(\pm\frac{1}{m+i}) \notin \mathbb{Z}$

2 Congruence

2.1 The Difinition and Property of Congruence

suppose a,b,q,r∈ℤ , a=bq+r , |r|<b, marked as a(mod b)=r

if a(mod p)=b(mod p) , it is called a and b are congruent , marked as a≡b(mod p)

Theorem:

(1)a≡b(mod p) ⇔ p|±(a-b)

(2)if a_1≡b_1(mod p) and a_2≡b_2(mod p) ⇔ $(a_1 \pm a_2)$≡$(b_1 \pm b_2)$(mod p)

(3)if a_1≡b_1(mod p) and a_2≡b_2(mod p) ⇔ $(a_1 a_2)$≡$(b_1 b_2)$(mod p)

(4)if am≡bm(mod p) and (m,p)=1 ⇔ a≡b(mod p)

(5)if a≡b(mod p) and d|p ⇔ a≡b(mod d)

Prove:

(1)(2)skip

(3)suppose

$$\begin{aligned}
a_1 &= q_{11}p + r_1 \\
b_1 &= q_{12}p + r_1 \\
a_2 &= q_{21}p + r_2 \\
b_2 &= q_{22}p + r_2 \\
a_1 a_2 &= q_{11}q_{21}p^2 + q_{21}r_1 p + q11r_2 p + r_1 r_2 \\
b_1 b_2 &= q_{12}q_{22}p^2 + q_{22}r_1 p + q12r_2 p + r_1 r_2 \\
\therefore a_1 a_2 &\equiv b_1 b_2 (mod p)
\end{aligned}$$

(4)

$$\because am \equiv bm(modp)$$
$$\therefore p \mid m(a-b)$$
$$\because (m,p) = 1$$
$$\therefore p \nmid m$$
$$\therefore p \mid (a-b)$$
$$\therefore a \equiv b(modp)$$

(5)

$$\because a \equiv b(modp)$$
$$d \mid p$$
$$\therefore a = q_1 p + r$$
$$b = q_2 p + r$$
$$p = qd$$
$$\therefore a = q_1 qd + r$$
$$b = q_2 qd + r$$
$$a \equiv b(modd)$$

Theorem:

∀N∈ℤ and p≥2

$$N = n_d p^d + \cdots + n_1 p^1 + n_0$$

n_i∈ℤ , $|n_i|$ <p , n_d≠0

2.2 Euler's Totient Function

φ(m)=|S| , S={ a | a∈ℤ , a<m , (a,m)=1 }

Theorem:

$$\varphi(m) = m\sum_{i=1}^{k}(1-\frac{1}{p_i}) \qquad m = \prod_{i=1}^{k} p_i^{a_i}$$

Prove:

$$\varphi(m) = |\{1, 2, 3, \cdots, m-2, m-1\} - \mathcal{D}(m) + \{1\}|$$
$$\varphi(m) = m - |\mathcal{D}(m)|$$
$$\mathcal{D}(m) = \{d|d = \prod_{i=1}^{k'} p_i^{a_i}\} \quad a_i = 0, 1, \cdots, a_k \quad k' = k$$
$$|\mathcal{D}(m)| = \prod_{i=1}^{k}(a_k + 1)$$

2.2.1 Euler Theorem

if (a,m)=1 ,then

$$a^{\varphi(m)} \equiv 1(modm)$$

Prove:

2.2.2 Fermat's Little Theorem

if p is a prime , ∀a∈ℤ

$$a^p \equiv a(modp)$$

Prove:

2.3 Exercise:

(1) if $a \equiv b(mod\ m_i)$, $i = 1, 2 \cdots n \ \Rightarrow \ a \equiv b(mod\ [m_1, \cdots, m_n])$

(2) if p, q are prime and $p \neq q \Rightarrow q^{p-1} + p^{q-1} \equiv 1(mod\ pq)$

(3) if $(a, b) = 1, c \neq 0 \Rightarrow \exists n, (a + nb, c) = 1$

3 Congruence Equation

3.1 Residue System

$\forall$n$\in\mathbb{Z}$, n≡r(mod p) $\Leftrightarrow$ n=qp+r , r=0,±1,±2,$\cdots$

let

$\overline{0}$={0,±p,±2p,$\cdots$}

$\overline{1}$={±1,1±p,1±2p,$\cdots$}

$\vdots$

$\overline{p-1}$={(p-1),(p-1)±p,(p-1)±2p,$\cdots$}

$\bar{i}$ is a residue class of n mod p

3.1.1 Complete Residue System

choose a number from each residue class to represent its residue class , all these numbers form a set , { $\overline{0},\overline{1},\cdots,\overline{p-1}$ } is a complete residue system of n mod p

3.1.2 Reduced Residue System

if { $1,j,\cdots,p-1$ }$\subset${ $\overline{0},\overline{1},\cdots,\overline{p-1}$ } , $\forall$a$\in${ $1,j,\cdots,p-1$ } , (a,p)=1 , then { $1,j,\cdots,p-1$ } is a reduced residue system of n mod p

|{ $1,j,\cdots,p-1$ }|=φ(p)

Theorem:

(1)if { $x_1,x_2,\cdots,x_{\varphi(m)}$} is a reduced residue system , (a,m)=1 $\Rightarrow$ { $ax_1,ax_2,\cdots,ax_{\varphi(m)}$} is a reduced residue system

3.2 Linear Congruence Equation

3.2.1 Linear Congruence Equation

ax≡b(mod m) is called linear congruence equation

$$\begin{aligned}
&\because ax \equiv b(mod\ m)\\
&\therefore m \mid (ax-b)\\
let\quad & ax-b=mq\\
&\therefore ax = mq+b\\
&\therefore x=\frac{m}{a}q+\frac{b}{a}\\
let\quad & a'=\frac{a}{(a,m)}\\
& m'=\frac{m}{(a,m)}\\
& (a',m')=1\\
if\quad & (a,m)\mid b\\
& b'=\frac{m}{(a,b)}\\
& m' \mid (a'x-b')\\
& a'x \equiv b'(mod\ m')\\
& x \equiv b'a'^{-1}(mod\ m')\\
& x = b'a'_{-1}+km' \qquad k=0,\pm1,\pm2,\cdots
\end{aligned}$$

$$\because a(\frac{b}{(a,m)}a'^{-1}+km')(mod\ m)=(a'a'^{-1}b+a'km)(mod\ m)=b(mod\ m)\quad k=0,1\cdots(a,m)-1$$

$$\therefore x \equiv a'^{-1}\frac{b}{(a,m)}+k\frac{m}{(a,m)}$$

Theorem:

(1)ax≡ b(mod m),(a,m)| b ⇔ x≡ $a'^{-1}\frac{b}{(a,m)}$+k$\frac{m}{(a,m)}$, k=0,1$\cdots$ (a,m)-1

3.2.2 Linear Congruence Equation Set

$$\begin{cases}
x \quad \equiv b_1(mod\ m_1)\\
x \quad \equiv b_2(mod\ m_)\\
\vdots\\
x \quad \equiv b_k(mod\ m_k)
\end{cases}$$

it is called linear congruence equation

3.2.3 Chinese Remainder Theorem

When (m_i, m_j)=1 , i≠j and i,j=1,2$\cdots$k

$$x \equiv M_1^{-1} M_1 b_1 + \cdots + M_k^{-1} M_k b_k$$

$$m = \prod_{i=1}^{k} m_i \qquad M_i = \frac{m}{m_i} \qquad M_i^{-1} M_i \equiv 1 (mod m_i)$$

Prove:

3.3 Polynomial Congruence Equation

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

$$\because (x^p - x) \equiv 0 (mod\ p)$$

$$f(x) \equiv (x^p - x) q(x) + r(x) (mod\ p)$$

$$\therefore f(x) \equiv r(x) (mod\ p)$$

/vspace12 pt **Theorem:** if the numbers of solution of

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

is n
then $f(x) | (x^p - x)$

3.4 Wilson Theorem

suppose p is a prime

$$(p-1)! + 1 \equiv 0 (mod\ p)$$

3.5 Exercise:

(1) $x \equiv 7(mod\ 10) \quad x \equiv 3(mod\ 12) \quad x \equiv 12(mod\ 15)$

(2) $3x^{14} + 4x^{13} + 2x^{11} + x^9 + x^6 + x^3 + 12x^2 + x \equiv 0(mod\ 7)$

4 Quadratic Residue

4.1 Difinition and Property of Quadratic Residue

if p is an odd prime and

$$x^2 \equiv a(mod\ p) \qquad (a,p) = 1$$

has a solution,then a is a quadratic residue of p , otherwise a is quadratic non-residue of p

Theorem:

(1)if p is an odd prime , there are $\frac{p-1}{2}$ quadratic residue and $\frac{p-1}{2}$ quadratic non-residue
(2)if p is an odd prime , (a,p)=1
a is a quadratic residue mod p $\Leftrightarrow a^{\frac{p-1}{2}} \equiv 1(modp)$
a is a quadratic non-residue mod p $\Leftrightarrow a^{\frac{p-1}{2}} \equiv -1(modp)$

Prove:

4.2 Legendre Symbol

if a is an odd prime , a∈ℤ

$$(\frac{a}{p}) = a^{\frac{p-1}{2}}(mod\ p) = \begin{cases} 1 & a\ is\ a\ quadratic\ residue\ mod\ p \\ -1 & a\ is\ not\ a\ quadratic\ residue\ mod\ p \\ 0 & p \mid a \end{cases}$$

Theorem:

$$(1) \quad (\frac{1}{p}) = 1\ ,\ (\frac{-1}{p}) = (-1)^{(\frac{p-1}{2})}$$

$$(2) \quad if \quad a \equiv b(mod\ p)\ \Leftrightarrow\ (\frac{a}{p}) = (\frac{b}{p})$$

$$(3) \quad (\frac{a+p}{p}) = (\frac{a}{p})$$

$$(4) \quad (a,p) = 1\ \Leftrightarrow\ (\frac{a^2}{p}) = 1$$

$$(4) \quad (\frac{a_1 a_2 \cdots a_n}{p}) = (\frac{a_1}{p})(\frac{a_2}{p}) \cdots (\frac{a_n}{p})$$

Prove:

Lemma:

$$(1) \quad (\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}}$$

4.2.1 Quadratic Reciprocity Law

if p,q are odd prime , (p,q)=1 , then

$$(\frac{q}{p}) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}(\frac{p}{q})$$

4.3 Jacobi Symbol

if m is an odd and m>1 , m=$p_1 p_2 \cdots p_r$, $p_i$is a prime , then

$$(\frac{a}{m}) = (\frac{a}{p_1})(\frac{a}{p_2}) \cdots (\frac{a}{m_r})$$

$p_1, p_2 \cdots p_r$ can be duplicate

Theorem:

$$(1) \quad (\frac{1}{m}) = 1$$

$$(2) \quad if\ a \equiv b(mod\ m) \ \Leftrightarrow \ (\frac{a}{m}) = (\frac{b}{m})$$

$$(3) \quad if\ (a, m) = 1 \ \Leftrightarrow \ (\frac{a^2}{m}) = 1$$

$$(4) \quad (\frac{a+m}{m}) = (\frac{a}{m})$$

$$(5) \quad (\frac{a_1 a_2 \cdots a_n}{m}) = (\frac{a_1}{m})(\frac{a_2}{m}) \cdots (\frac{a_n}{m})$$

$$(6) \quad (\frac{-1}{m}) = (-1)^{\frac{m-1}{2}}$$

$$(7) \quad (\frac{2}{m}) = (-1)^{\frac{m^2-1}{8}}$$

$$(8) \quad if\ m,n>1\ and\ m\ ,\ n\ is\ odd\ prime\ \Rightarrow\ (\frac{n}{m})=(-1)^{\frac{m-1}{2}\frac{n-1}{2}}(\frac{m}{n})$$

Prove:

4.4 Exercise:

(1)if p is an odd prime , $p\equiv 1(mod\ 4)\Rightarrow$

in $1,2\cdots\frac{p-1}{2}$, there are $\frac{p-1}{4}$ quadratic residue and non-quadratic residue

5 Discrete Logarithm

5.1 Index and Primitive Root

if d>0 and d$\in\mathbb{Z}$

$$a^d\equiv 1(mod\ p)$$

d_{min} is called index of a mod p , marked as $ord_m(a)$

if

$$ord_m(a)=\varphi(m)$$

then a is a primitive root mod m

Theorem:

$$(1) \quad if\ a\equiv b(mod\ m)\ \Rightarrow\ ord_m(a)=ord_m(b)$$

$$(2) \quad a^d\equiv 1(mod\ m)\ \Leftrightarrow\ ord_m(a)\mid d$$

$$(3) \quad ord_m(a)\mid\varphi(m)$$

$$(4) \quad if\ a^{-1}a\equiv 1(mod\ m)\ \Rightarrow\ ord_m(a^{-1})=ord_m(a)$$

$$(5) \quad a^d\equiv a^k(mod\ m)\ \Rightarrow\ d\equiv k(mod\ ord_m(a))$$

$$(6) \quad if\ k > 0\ and\ k \in \mathbb{Z}\ \Rightarrow\ ord_m(a^k) = \frac{ord_m(a)}{(ord_m(a), k)}$$

$$(7) \quad if\, there\, is\, a\, primitive\, root\, mod\, m\ ,\ and\, there\, are\, \varphi(\varphi(m))\, primitive\, roots\, in\, total$$

$$(8) \quad ord_m(ab) = ord_m(a)ord_m(b)\ \Leftrightarrow\ (ord_m(a), ord_m(b)) = 1$$

$$(9) \quad if\ n \mid m\ \Rightarrow\ ord_m(a) \mid ord_m(a)$$

$$(10) \quad if\ (m_1, m_2) = 1\ \Rightarrow\ ord_{m_1 m_2}(a) = [ord_{m_1}(a), ord_{m_2}(a)]$$

Prove:

5.2 Existence of Primitive Root

Theorem:

$$(1) \quad if\ p\ is\ an\ odd\ prime\ ,\ then\ there\ are\ primitive\ roots\ mod\ p$$

$$(2) \quad there\, are\, primitive\, roots\, mod\, m\ \Leftrightarrow\ m = 2, 4, p^{\alpha}, 2p^{\alpha} \qquad p\, is\, an\, odd\, prime$$

(3) suppose the different divisors of φ(m) is $q_1, q_2 \cdots q_k$ and (g,m)=1 , g is a primitive root $\Leftrightarrow g^{\frac{\varphi(m)}{q_i}} \neq 1(mod\ p)$, i=1,2$\cdots$ k

Prove:

5.3 Discrete Logarithm

if g is a primitive root mod m , ∀a∈$\mathbb{Z}$, (a,m)=1

$$a \mid g^{\gamma}(mod\ m) \qquad 0 \leq \gamma \leq \varphi(m)$$

γ is a discrete logarithm , marked as $ind_g a$

Theorem:

$$(1) \quad ind_g 1 = 0, ind_g g = 1$$

$$(2) \quad ind_g(ab) \mid ind_g a + ind_g b\ (mod\ \varphi(m))$$

$$(3) \quad ind_g a^n \mid n \cdot ind_g a\ (mod\ \varphi(m)) \qquad n \geq 1$$

$$(4) \quad if\, g\, and\, g'\, are\, primitive\, roots\, mod\, m\ \Rightarrow ind_g a \mid ind_{g'} a{\cdot}ind_g g'\ (mod\, \varphi(m))$$