3. Mathematical Backgrounds.

3.1. Information Theory

In 1949, Shannon provides a theoretical foundations for cryptography based on his fundamental work on information theory. He measured the theoretical secrecy of a cipher by the uncertainty about the plaintext given the received ciphertext. If, no matter how much ciphertext is intercepted, nothing can be learned about the plaintext, the cipher achieves ***perfect secrecy***.

<u>Entropy and Equivocation</u>

Information theory measures the amount of information in a message by the average number of bits needed to encoded all possible messages in an optimal encoding. The Sex field in a database, for example, contains only one bit of information because it can be encoded with one bit (Male can be represented by "0", Female by "1"). If the field is represented by an ASCII character encoding of the character strings "MALE" and "FEMALE", it will take up more space, but will not contain any more information.

The amount of information in a message is formally measured by the entropy of the message. The entropy is a function of the probability distribution over the set of all possible messages. Let $X_1,\ldots, X_n$ be n possible messages occurring with probabilities $p(X_1),\ldots,p(X_n)$, the sum of this probabilities $p(X_i), i=1,\ldots,n$ equals to one. The entropy of a given message is defined by the weighted average:

$$H(X)=-\sum_i^n p(X_1) \log_2 p(X_1).$$

As the sum taken over all messages X:

$$H(X)=-\sum_X p(X) \log_2 p(X)=\sum_X p(X) \log_2 [1/p(X)].$$

3. Mathematical Backgrounds.

3.2. Information theory in Examples

Intuitively, each term $log_2\ [1/p(X)]$ in last expression represents the number of bits needed to encode message X in an optimal encoding that is, one which minimizes the expected number of bits transmitted over the channel. The weighted average H(X) gives the expected number of bits in optimally encoded messages.

Because $1/p(X)$ decrease as $p(X)$ increase, an optimal encoding uses short codes for frequently occurring messages at the expense of using longer ones for infrequently messages. This principle is applied in ***Morse code***, where the most frequently used letters are assigned the shortest codes.

"Huffmen Code" are optimal codes assigned to characters, words, machine instructions, or phases. Single – character ***Huffmen*** code are frequently used to compact large files. COMPACT program on UNIX reduced its storage requirements by 38%, which is typical for text files.

Example 3.2.1. Let $n=3$, and let the 3 messages be the letters $A,B,$ and C, where $p(A)=1/2$ and $p(B)=p(C)=1/4$. Then

$$log_2(1/\ p(A))=log_2 2= 1;$$

$$log_2(1/\ p(B))=log_2(1/\ p(C))=log_2 4= 2;$$

what confirming our earlier observation, that for frequently occurring message the minimal number of bits is needed for optimal encoding.

2. Mathematical Backgrounds

2.2. Information theory in Examples

Example 3.2.2. Suppose there are two possibilities: *Mail* and *Female*, both equally likely; thus $p(Male)=p(Female)=1/2$. Then

$$H(X)=p(Male)log_2(1/\,p(Male))+ p(Female)log_2(1/\,p(Female))=$$
$$=(1/2)(log_2 2)+(1/2)(log_2 2)= 1,$$

what confirming our earlier observation that there is 1 bit of information in the *Sex* field of a database.

The following example illustrate the application of entropy to determine the information content of a massage.

Example 3.2.3. Let $n=3$, and let the 3 messages be the letter $A,B,$and C, where $p(A)=1/2,\ p(B)=p(C)=1/4$. Then

$$H(X)=(1/2)log_2 2+2(1/4)log_2 4=0.5+1.0=1.5.$$

An optimal encoding assigns a 1-bit code to *A* and 2-bit codes to *B* and *C*. For example, *A* can encoded with the bit 0, while B and C can be encoded with two bits each, 10 and 11. Using this encoding, the 8-letter sequence ABCAABAC is encoded as the 12-bit sequence 010110010011 as shown next:

A	B	C	A	A	B	A	C
0	10	11	0	0	10	0	11

The average number of bits per letter is 12/8=1,5.

3. Mathematical Backgrounds

3.2. Information theory in Examples

For a given language, consider the set of all messages N character long. The ***rate of the language for messages of length N*** is defined by

$$r=H(X)/N,$$

That is, the average number of bits of information in each character.

The simplest solution to determine the rate of language (***absolute rate R***) based on the assumption that all letters have the same probability of occurring within the all possible messages, as well as all possible sequences of characters are equally likely. If there are L characters in the language, then the absolute rate is given by

$$R=\log_2 L,$$

For English language this probability is equal to $L=26$, then $R=\log_2 L=\log_2 26 =4{,}7 bit/letter$.

The absolute rate of the language is defined to be the maximum number of bits of information that could be encoded in each character.

The actual rate of English is thus considerably less than its absolute rate. The reason is that English, like all natural languages, is highly redundant. For example, the phrase “occurring frequently” could be reduced by 58% to “crng frg” without loss of information.

3. Mathematical Backgrounds

3.2. Information theory in Examples

1.Single letter frequency distributions.

A	0.0804	H	0.0549	O	0.0760	V	0.0099
B	0.0154	I	0.0726	P	0.0200	W	0.0192
C	0.0306	J	0.0016	Q	0.0011	X	0.0019
D	0.0399	K	0.0067	R	0.0612	Y	0.0173
E	0.1251	L	0.0414	S	0.0654	Z	0.0009
F	0.0230	M	0.0253	T	0.0925		
G	0.0196	N	0.0709	U	0.0271		

Then $r=H(1\text{-grams})/1=4.15$.

2.Diagrams frequency distributions. Certain diagrams (pair of letters) such as *TH* and *EN* occur much more frequently than others. Some diagrams (e.g., OZ) never occur in meaningful messages (acronyms are on exception). Then $r=H(2\text{-grams})/2=3.62$.

3.Trigrams frequency distributions. The proportion of meaningful sequences decreases when trigrams are considered (e.g. BB is meaningful but BBB is not). Such as THE and ING occur much more frequently than others. Then $r=H(3\text{-grams})/2=$ $=3.22$.

The rate of a language (entropy per character) is determined by estimating the entropy of N-grams for increasing values of N. As N increases, the entropy per character decreases because there are fewer choices and certain choices are much more likely. For $N\to\infty$,$r=1\div 1,5$.

The redundancy of a language with rate r and absolute rate R is defined by $D=R-r$. For $R=4.7$ and rate $r=1$, $D=3.7$, whence the ratio D/R shows English to be about 79% redundant; for $r=1.5$, $D=3.2$, implying a redundancy of 68%.

3. Mathematical Backgrounds

3.3. Perfect Secrecy

Shannon studied the information theoretic properties of cryptographic systems in terms of three classes of information:

1. Plaintext messages M occurring with prior probabilities $p(M)$, where $\Sigma_M p(M)=1$.

2. Ciphertext messages C occurring with prior probabilities $p(C)$, where $\Sigma_C p(C)=1$.

3. Keys K occurring with prior probabilities $p(K)$, where $\Sigma_K p(K)=1$.

Let $p_c(M)$ be the probability that message M was sent given that C was received (thus C is the encryption of message M). ***Perfect secrecy*** is defined by the condition.

$$p_C(M)=p(M)$$

That is, intercepting the ciphertext gives a cryptanalyst no additional information.

A necessary and sufficient condition for perfect secrecy is that for every C,

$$p_M(C)=p(C) \text{ for all } M,$$

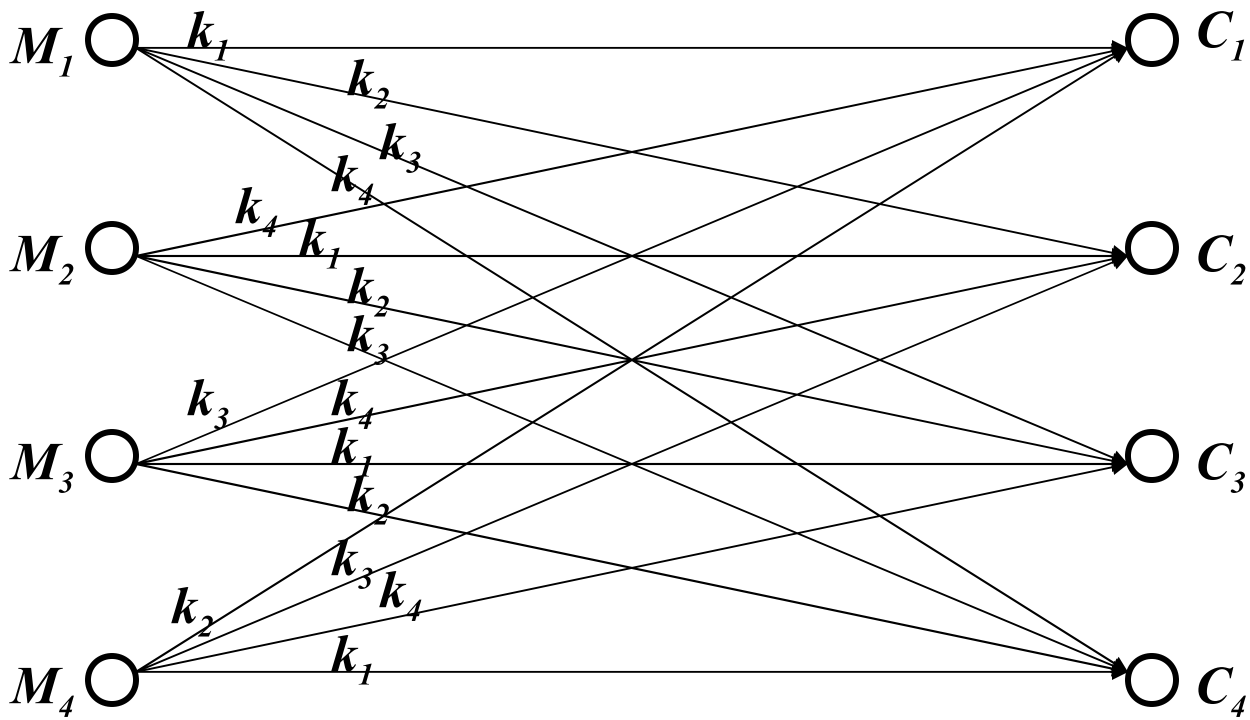
This means the probability of receiving a particular ciphertext C given that M was sent (enciphered under the same key) is the same as the probability of receiving C given that some other message M' was sent (enciphered under a different key).

Perfect secrecy is possible using completely random keys at least as long as the messages they encipher.

3. Mathematical Backgrounds

3.3. Perfect Secrecy

Next figure illustrates a perfect secrecy system with four messages, all equally likely, and four keys, also equally likely.



Here $p_C(M)=p(M)=1/4,$ and $p_M(C)=p(C)=1/4$ for all M and C. A cryptoanalyst intercepting one of the ciphertext messages $\boldsymbol{C_1}$ $\boldsymbol{C_2}$ $\boldsymbol{C_3}$ or $\boldsymbol{C_4}$ would have no way of determining which of the four keys was used and, therefore, whether the correct message is $\boldsymbol{M_1}$ $\boldsymbol{M_2}$ $\boldsymbol{M_3}$ or $\boldsymbol{M_4}$

3. Mathematical Backgrounds

3.3. Perfect Secrecy

Perfect secrecy requires that the number of keys must be at least as great as the number of possible messages. Otherwise there would be some message M such that for given C, no K decipher C into M, implying $p_C(M)=0$. The cryptanalyst could thereby eliminate certain possible plaintext message from consideration, increasing the chances of breaking the cipher.

A cipher using a nonrepeating random key stream such as the one described in the preceding example is called a ***one-time pad***.One-time pads are the only ciphers that achieve perfect secrecy.

The implementation of one-time pads in computer systems is based on an ingenious device designed by Gilbert Verman in 1917. Letting $M=m_1m_2...$ denotes a plaintext bit stream and $K=k_1k_2...$ a key bit stream, the Verman cipher generates a ciphertext bit stream $C=E_K(M)=c_1c_2...$, where $c_i=(m_i+k_1)$ mod 2, $i=1,2,...$. The Verman cipher is efficiently implemented in microelectronics by taking the "exclusive-or" of each plaintext/key pair $c_i=m_i+k_i$ Because $k_i+k_i=0$ for $k_i=0$ or 1, deciphering is performed with the same operation: $c_i+k_i = m_i+k_i + k_i=m_i$.

Example 3.2.4. *M=0111001101010101, K=0101011100101011,* here the key stream represent the stream of random bits with probabilities $p(0)=p(1)=0.5$.

Enciphering procedure: $C=M\oplus K=0111001101010101\oplus$ $\oplus\, 0101011100101011=0010010001111110.$

Deciphering procedure: $M=C\oplus K=0010010001111110\oplus$ $\oplus\, 0101011100101011= 0111001101010101.$

3. Mathematical Backgrounds

3.4.Complexity Theory

The strength of a cipher is determined by the computational complexity of the algorithms used to solve the cipher. The computational complexity of an algorithm is measured by its time *T* and space *S* requirements are expressed as function *f(n)* of *n*, and *n* characterized the size of the input. This function is typically bounded as an "order-of-magnitude" of the form $O(n^t)$, where *t* can take any constant value.

For example if *f(n)* is a polynomial of the form $f(n)= a_t n^t + a_{t-1} n^{t-1} + \ldots + a_1 n^1 + a_0$ for constant *t,* then $f(n)= O(n^t)$; that is, all constants and low-order terms are ignored.

Measuring the time and space requirements of an algorithm by its order-of-magnitude allows to see how the time and space requirements grows as the size of the input increases. For example, if $T= O(n^2)$, doubling the size of the input quadruples the running time. Table 2.4.1 shows the running times of different classes of algorithms for $n=10^6$.

Class	Complexity	Number of operations for $n=10^6$	Real time
Polynomial			
Constant	$O(1)$	1	*1 µsec*
Linear	$O(n)$	10^6	*1 second*
Quadratic	$O(n^2)$	10^{12}	*10 days*
Cubic	$O(n^3)$	10^{18}	*27397 years*
Exponential	$O(2^n)$	10^{301030}	*10^{301016} years*

3. Mathematical Backgrounds

3.4.Complexity Theory

Complexity theory classifies a problem according to the minimum time and space needed to solve the hardest instances of the problem based on some abstract model of computation.

The class ***P*** consists of all problems solvable in polynomial time.

The class ***NP*** (nondeterministic polynomial) consists of all problems solvable in polynomial time on nondeterministic model of computation.

The class ***NP-complete*** has the property that if any one of the problems is in ***P***, then all ***NP*** problems are in ***P*** and ***P=NP***. Thus the ***NP-complete*** problems are the "hardest" problem in ***NP***. The fastest known algorithms for systematically solving these problems have worst-case time complexities exponential in the size n of the problem.

It have been shown that ***NP-complete*** problems might make excellent candidates for ciphers because they cannot be solved (systematically) in polynomial time by any known techniques. ***NP-complete*** problems could be adapted to cryptographic use. To construct such a cryptographic system, secret "***trapdoor***" information is inserted into a computationally hard problem that involves inverting a one-way function.

A function f is a ***one-way function*** if it is easy to compute $f(x)$ for any x in the domain of f, while, for almost all y in the range of f, it is computationally infeasible to compute $f^{-1}(y)$ even if f is known. It is a ***trapdoor one-way function*** if it is easy to compute $f^{-1}(y)$ given certain additional information. The additional information, usually is the secret deciphering key.

3. Mathematical Backgrounds

3.5. Number Theory

The set of ***Natural Numbers*** is divided into two subset: ***Real Number*** and ***Integer Numbers.*** The main subset of numbers to be used in the field of Data Security is the Integer Numbers.

Integer Number d is a divider of n if and only if $n=kn$. It can be notated as $d \mid n$. If there is no any k, d is not a divider of n, what can be expressed as $d \nmid n$.

Integer number p, $p>1$ is the prime number if the only dividers for this number are 1 and p.

Theorem 3.5.1. *(Euclid's)* There is infinite set of prime numbers.

Proof: Suppose that this set is finite and consists of the prime numbers p_1, p_2, p_3, …,p_k. Then it is the contradiction that the number

$$\left(\prod_{i=1}^{k} p_i\right) + 1,$$

is not divided by any of prime number p_1, p_2, p_3, …,p_k, thus it is divided by 1 and itself, what means that this number is a prime number. #

Theorem 2.3.2. For any big positive integer number $k \geq 1$, there is a possibility to determine k composite numbers, following in a row within the set of integer numbers.

Proof: The number $(k+1)!=2 \cdot 3 \cdot 4 \cdot \ldots \cdot (k+1)$ is divided by any of the following numbers $2,3,4,\ldots,(k+1)$. Thus, the numbers following in a row within the set of integer numbers $(k+1)!+2$, $(k+1)!+3$, $(k+1)!+4$, …, $(k+1)!+(k+1)$, are composite numbers due to the fact that first number is divided by 2, second by 3 and so on. #

3.5. Number Theory

Theorem 3.5.3. If the integer number $n (n>1)$ is not divided by any prime number no greater than $\sqrt{n}$ means that it is a prime number.

Proof: Suppose that n is a composite number, and can be expressed as $n=ab,\ 1<a<n;\ 1<b<n$. Numbers a and b can not be greater than $\sqrt{n}$ simultaneously. #

Theorem 3.5.4. (Eratosfen's)

1) If in a set of integer numbers $2,3,4,..,N,$ delete all numbers divided by the first r prime numbers $2,3,5,7,\ldots,p_r,$ then the first is not deleted number is a prime number.

2) If in a set of integer numbers $2,3,4,..,N$, delete all numbers divided by the prime numbers less or equal to $\sqrt{N}$, such a way that $p_r \le \sqrt{N} \le p_{r+1}$, then all remaining numbers will be the prime numbers p within the set $\sqrt{N} < p \le N.$

2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

	3		5		7		9		11		13		15		17		19		21		23		25	

			5		7				11		13				17		19				23		25	

					7				11		13				17		19				23			

3. Mathematical Backgrounds

3.5. Number Theory

The distribution of Primes

At the present, the most practical method of selecting primes suitable for use in the RSA algorithm is to test randomly selected integers until the required number of primes have been found. The approach works only because the propagation of primes to nonprimes is high enough.

By actual count, one finds that each group of 100 numbers, from 1 to 1000 (1 to 100, 101 to 200, etc.) contains respectively, the following number of primes: 25,21,16,16,17,14,16,14,15,14. In each group of 100 numbers from 1,000,001 to 1,001,000, the corresponding frequency of primes is: 6,10,8,8,7,7,10,5,6,8, and from 10,000,001 to 10,001,000 the corresponding frequency is 2,6,6,6,5,4,7,10,9,6.

According to the ***prime number theorem***, the ratio of $\pi(x)$, the number of primes in the interval from 2 to x and $x/ln(x)$ approaches 1 as x becomes very large, that is

$$\lim_{x \to \infty} \frac{\pi(x)}{x/\ln(x)} = 1$$ Where $ln(x)$ is the (natural) logarithm of x.

x	$\pi(x)$	$x/ln(x)$	$\lim_{x \to \infty} \frac{\pi(x)}{x/\ln(x)}$
1,000	168	145	1.159
100,000	9,592	8,686	1.104
10,000,000	664,579	620,421	1.071
1,000,000,000	50,847,476	48,254,942	1.054

3. Mathematical Backgrounds

3.5. Number Theory

Fermat's prime numbers: *3,5,17,257,65537*, generated by the equation

$$2^{2^k}+1.$$

Euler's prime numbers can be generated according to the equation x^2-x+41, foe all integer *x*, $0 \le x \le 40$.

Mercen's prime numbers can be generated according to 2^n-1
For prime *n=2,3,5,7,13,17,19,31,61*.

The greatest known prime number is a Mercen's number $2^{1398269}$ with *420921* digits.

Composite numbers can be represented in a canonical form

$$a=\prod_{i=1}^{k} p_i^{\alpha_i}$$

where p_i are the prime numbers.

Example 3.5.5. $a=120=2^3\cdot 3^1\cdot 5^1$

Common Divisor of the numbers $a_1,a_2,a_3,\dots,a_n$, is an integer *d,* that $d\,|\,a_1$, $d\,|\,a_2$, $d\,|\,a_3$, …, $d\,|\,a_n$.

Greatest Common Divisor of the numbers $a_1,a_2,a_3,\dots,a_n$, is a greatest integer divisor *d,* that can be divided by any common divisor of this numbers $(a_1,a_2,a_3,\dots,a_n)=d$.

Example 3.5.6. *(6,15,27)=3.*

3. Mathematical Backgrounds

3.5. Number Theory

Theorem 3.5.5. If

$$a_1 = \prod_{i=1}^{k} p_i^{\alpha_i} \quad a_2 = \prod_{i=1}^{k} p_i^{\beta_i} \quad \ldots \quad a_n = \prod_{i=1}^{k} p_i^{\gamma_i}$$

then the greatest common divisor (g.c.d.) is

$$(a_1, a_2, \ldots, a_n) = \prod_{i=1}^{k} p_i^{\min\{\alpha_i, \beta_i, \ldots, \lambda_i\}}$$

Example 3.5.5. If $6=2^1 \cdot 3^1$, $15= 3^1 \cdot 5^1$, $27= 3^3$, then $(6,15,27)=$
$=2^{\min\{1,0,0\}} \cdot 3^{\min\{1,1,3\}} \cdot 5^{\min\{0,1,0\}} = 2^0 \cdot 3^1 \cdot 5^0 = 3.$

Theorem 3.5.6. If

$$a_1 = \prod_{i=1}^{k} p_i^{\alpha_i} \quad a_2 = \prod_{i=1}^{k} p_i^{\beta_i} \quad \ldots \quad a_n = \prod_{i=1}^{k} p_i^{\gamma_i}$$

then the least common multiplier (l.c.m.) is

$$l.c.m.(a_1, a_2, \ldots, a_n) = \prod_{i=1}^{k} p_i^{\max\{\alpha_i, \beta_i, \ldots, \lambda_i\}}$$

Example 3.5.6. If $6=2^1 \cdot 3^1$, $15= 3^1 \cdot 5^1$, $27= 3^3$, then $l.c.m.(6,15,27)=$
$=2^{\max\{1,0,0\}} \cdot 3^{\max\{1,1,3\}} \cdot 5^{\max\{0,1,0\}} = 2^1 \cdot 3^3 \cdot 5^1 = 270.$

3.5. Number Theory

Theorem 3.5.7. If $a=bq+r$, then $(a,b)=(b,r)$.

Proof: Let $d=(a,b)$, then from the statement that $d \mid a$ and $d \mid b$ we can conclude that d is a divider for $a-bq=r$.#

Theorem 3.5.8. (Euclid Algorithm) For any integer numbers $a>0$ and $b>0$ that $a>b$, and b is not a divider of a for some s exists integer numbers $q_0, q_1, q_2, \ldots, q_s$ and $r_0, r_1, r_2, \ldots, r_s$ that $b>r_0>r_1>r_2>\ldots>r_s>0$ and $a=bq_0+r_1$, $b=r_1q_1+r_2$, $r_1= r_2q_2+r_3, \ldots$, $r_{s-2}= r_{s-1}q_{s-1}+r_s$, $r_{s-1}= r_sq_s$ and $(a,b)=r_s$

Euclid's Algorithm

begin

$g_0:=a;$

$g_1:=b;$

while $g_i \neq 0$ ***do***

begin

$g_{i+1}:= g_{i-1} \bmod g_i;$

$i:=i+1;$

end

$gcd:= g_{i-1}$ *{gcd-Greatest Common Divisor}*

end

3.5. Number Theory

Example 3.5.7. Determine the greatest common divisor for integers *1173* and *323, (1173,323)=?*.

Solution: $1173=323\cdot 3+204$; $323=204\cdot 1+119$; $204=119\cdot 1+85$; $119=85\cdot 1+34$; $85=34\cdot 2+17$; $34=17\cdot 2$;

$$\mathbf{g_{i+1} := g_{i-1} \bmod g_i;}$$
$$204 := 1173 \bmod 323;$$
$$119 := 323 \bmod 204;$$
$$85 := 204 \bmod 119;$$
$$34 := 119 \bmod 85;$$
$$17 := 85 \bmod 34;$$
$$0 := 34 \bmod \mathbf{17}.$$

Binary Algorithm This algorithm is an extension of Euclid's Algorithm and is based on the following statements: 1. If both *a* and *b* are even, then $(a,b)=2(a/2,b/2)$; 2.If *a* even, and *b* odd, then $(a,b)=(a/2,b)$; 3.According to the Theorem 2.5.7 $(a,b)=(b,a-b)$; 4.If both *a* and *b* are odd, then $a-b$ is even.

Example 3.5.8. Determine the greatest common divisor for integers *1173* and *323, (1173,323)=?*.

Solution: $(1173,323)=(323,850)=(323,425)=(323,102)=(323,51)=(51,272)=(51,136)=(51,68)=(51,34)=(51,17)=(17,34)=(17,17)=17$.

3. Mathematical Backgrounds

3.5. Number Theory

Numbers $a_1, a_2, a_3, \ldots, a_n$, are ***relatively prime*** if and only if $(a_1, a_2, a_3, \ldots, a_n)=1$.

Numbers $a_1, a_2, a_3, \ldots, a_n$, are ***pair wise relatively prime*** if and only if for any i and $j \neq i$ $(a_i, a_j)=1$.

Theorem 3.5.9. If $(a,b)=1$, then for any integer numbers n and m $(a^n, b^m)=1$, as well as, if $(a^n, b^m)=1$, for any integer numbers n and m then $(a,b)=1$.

Proof: If $(a,b)=1$, then if canonical representation of $a=p_1^{\alpha 1}, p_2^{\alpha 2}, \ldots, p_k^{\alpha k}$ has $\alpha i>0$ it means that $\gamma i=0$ for canonical representation for $b=p_1^{\gamma 1}, p_2^{\gamma 2}, \ldots, p_k^{\gamma k}$, as well as in a case of $n\alpha i>0$ we have $\gamma i=0$. #

CONGRUENCES

Two integer numbers a and b are said to be congruent ***modulo*** m, if the difference $a-b$ is divided by m, what can be written as:

$$a \equiv b \ \mathbf{mod} \ m.$$

Last expression is called ***congruence.***

Example 3.5.9. $32 \equiv 5$ **mod** 9; $48 \equiv 12$ **mod** 9; $17 \equiv 7$ **mod** 5.

In a case when $b<m$, the b is a ***residue*** of a by ***modulo*** m.

3. Mathematical Backgrounds

3.5. Number Theory

There are a set of useful lemmas for congruence:

1. If $a \equiv b$ ***mod*** m, then for any integer k we have $ka \equiv kb$ ***mod*** m.
2. If $ka \equiv kb$ ***mod*** m, and $(k,m)=1$, then $a \equiv b$ ***mod*** m.
3. If $ka \equiv kb$ ***mod*** km, where k and m are any integer numbers then $a \equiv b$ ***mod*** m.
4. If $a \equiv b$ ***mod*** m, and $c \equiv d$ ***mod*** m, then $a+c \equiv b+d$ ***mod*** m.
5. If $a_1 \equiv b_1$ ***mod*** m, and $a_2 \equiv b_2$ ***mod*** m,…, $a_n \equiv b_n$ ***mod*** m, then $a_1+a_2+a_3+\ldots+a_n \equiv b_1+b_2+b_3+\ldots+b_n$ ***mod*** m.
6. If $a \equiv b$ ***mod*** m, and $c \equiv d$ ***mod*** m, then $a \cdot c \equiv b \cdot d$ ***mod*** m.
7. If $a_1 \equiv b_1$ ***mod*** m, and $a_2 \equiv b_2$ ***mod*** m,…, $a_n \equiv b_n$ ***mod*** m, then $a_1 \cdot a_2 \cdot a_3 \cdot \ldots \cdot a_n \equiv b_1 \cdot b_2 \cdot b_3 \cdot \ldots \cdot b_n$ ***mod*** m.
8. If $a \equiv b$ ***mod*** m, then for any integer $k>0$ we have $a^k \equiv b^k$ ***mod*** m.

3. Mathematical Backgrounds

3.5. Number Theory

Principle of Modular Arithmetic:

Modular arithmetic is based on the following theorem:

$(a*b) \textbf{ mod } m = [(a \textbf{ mod } m)*(b \textbf{ mod } m)] \textbf{ mod } m.$

Where $*$ is any of the following operations "+", "-" or "·".

The preceding theorem shows that evaluating $(a*b)$ ***mod*** m in modular arithmetic gives the same result as evaluating it in ordinary integer arithmetic and reducing the result ***mod*** m.

Example 3.5.10. $7 \cdot 9 \textbf{ mod } 5 = [(7 \textbf{ mod } 5) \cdot (9 \textbf{ mod } 5)] \textbf{ mod } 5.$

Note that the principle of modular arithmetic also applies to exponentiations because exponentiation is equivalent to repeated multiplications:

Example 3.5.11. Consider the expression 3^5 ***mod*** *7*. This can be computed by rising *3* to the power *5* and then reducing the result ***mod*** *7* as shown next:

1.Square 3:	3·3=9
2.Square the result:	9·9=81
3.Multiply by 3:	81·3=243
4.Reduce ***mod*** *7:*	243 ***mod*** *7*=5.

Alternatively, the intermediate results of the computations can be reduce ***mod*** *7*.

1.Square3:	3·3 ***mod*** 7=2
2.Square the result:	2·2 ***mod*** 7=4
3.Multiply by 3:	4·3 ***mod*** 7=5.

3. Mathematical Backgrounds

3.5. Number Theory

Fast Exponentiation Algorithm

```
begin "return x=a^z mod m"
        a_1:=a; z_1:=z;
        x:=1;
        while z_1≠0 do "x(a_1^z1 mod m)=a^z mod m"
                begin
                        while z_1 mod 2=0 do
                                begin "square a_1 while z_1 is even"
                                z_1:= z_1 div 2;
                                a_1:= (a_1· a_1) mod m;
                                end;
                        z_1:= z_1–1;
                        x:=(x·a_1) mod m "multiply"
                end;
                fastexp:=x;
end
```

3. Mathematical Backgrounds

3.5. Number Theory

Example 2.5.12. Consider the the calculation of $x = 5^{10}$ ***mod*** $7 = 5^{(1010)}$ ***mod*** 7. This can be computed by the *Fast Exponentiation Algorithm*.

$a_1 := 5;\ z_1 := 10;\ x := 1;$

$z_1 \neq 0;\ (10 \neq 0);$

$z_1 \bmod 2 = 0;\ (10 \bmod 2 = 0);$

$z_1 \operatorname{div} 2 = 5;\ (10/2 = 5);$

$a_1 := a_1 \cdot a_1 \bmod m = 4;\ (5 \cdot 5 \bmod 7 = 4);$

$z_1 \bmod 2 \neq 0;\ (5 \bmod 2 \neq 0);$

$z_1 := z_1 - 1 = 4;\ (5 - 1 = 4);$

$x := (x \cdot a_1) \bmod m = 4;\ (1 \cdot 4 \bmod 7 = 4);$

$z_1 \neq 0;\ (4 \neq 0);$

$z_1 \bmod 2 = 0;\ (4 \bmod 2 = 0);$

$z_1 \operatorname{div} 2 = 2;\ (4/2 = 2);$

$a_1 := a_1 \cdot a_1 \bmod m = 2;\ (4 \cdot 4 \bmod 7 = 2);$

$z_1 \neq 0;\ (2 \neq 0);$

$z_1 \bmod 2 = 0;\ (2 \bmod 2 = 0);$

$z_1 \operatorname{div} 2 = 1;\ (2/2 = 1);$

$a_1 := a_1 \cdot a_1 \bmod m = 4;\ (2 \cdot 2 \bmod 7 = 4);$

$z_1 \bmod 2 \neq 0;\ (1 \bmod 2 \neq 0);$

$\boldsymbol{5^2 \bmod 7 = 4;}$

$\boldsymbol{5^4 \bmod 7 = 4 \cdot 4 \bmod 7 = 2;}$

$\boldsymbol{5^8 \bmod 7 = 2 \cdot 2 \bmod 7 = 4;}$

$\boldsymbol{5^{10} \bmod 7 = 4 \cdot 4 \bmod 7 = 2.}$

3. Mathematical Backgrounds

3.5. Number Theory

If $a=r$ **mod** m, $(0<r<m)$, then $m \mid (a-r)$. Hence, there is $a-r=qm$ or $a=qm+r$. The remainder r is called a ***residue*** of a $(mod\ m)$. A set of m integers $\{a_i\}=\{a_1, a_2, ..., a_m\}$ is said to form a complete set of m integers in congruent ***modulo*** m for any r_i in the residue system $\{0,1,2,...,m-1\}$ in some order. This set is called ***Complete Residue System modulo m.*** Thus, for any integer a, there exists a congruence

$$a=r\ mod\ m$$

where r is a unique one among the numbers in a complete set of residues.

Example 2.5.13. The set of integer numbers $\{16,12,19,48,65\}$ is a complete residue system modulo 5. Really, $16=1\ mod\ 5$, $12=2\ mod\ 5$, $19=4\ mod\ 5$, $48=3\ mod\ 5$, $65=0\ mod\ 5$ and we have got complete set of residues $\{0,1,2,3,4\}$.

A set of integers $\{a_i\}=\{a_1, a_2, ..., a_n\}$ is said to form the ***residue class modulo m*** if all residues for a given numbers are the same and is equal r.

Example 2.5.14. The set of integer numbers $\{16,21,56,91,106\}$ is residue class modulo 5. Really, $16=1\ mod\ 5$, $21=1\ mod\ 5$, $56=1\ mod\ 5$, $91=1\ mod\ 5$, $106=1\ mod\ 5$ and we have got the same residue 1.

3. Mathematical Backgrounds

3.5. Number Theory

Fermat's Theorem. If p is a prime number and $(a,p)=1$, where a is an integer, then

$$a^{p-1}=1 \textbf{ mod } p.$$

Proof: For a given p and a, $(a,p)=1$ let consider $p-1$ positive products $a, 2a, 3a, \ldots, (p-1)a$. Any pair ia, ja $(i \neq j)$ of the products is not comparable by *modulo* p, namely

$$ia \neq ja \text{ mod } p,$$

what follows from the lemma for congruence's (see slide N 18).

As the result every product has their own unique nonzero residue r_i, $(1 \leq r_i \leq p-1)$. This residues $\{1,2,3,\ldots,(p-1)\}$ are in some order and create the Complete Residue System. Where $a=r_\alpha \text{mod } p$, $2a=r_\beta \text{mod } p$, $3a=r_\chi \text{mod } p, \ldots, (p-1)a=r_\lambda \text{mod } p$, where $\{r_\alpha, r_\beta, r_\chi, \ldots, r_\lambda\}=\{1,2,3,\ldots,(p-1)\}$. Based on the lemma for congruence (see slide N 18) we can get the product for the last congruence $a=r_\alpha \text{mod } p$, $2a=r_\beta \text{mod } p$, $3a=r_\chi \text{ mod } p, \ldots, (p-1)a=r_\lambda \text{mod } p$ as

$a \cdot 2a \cdot 3a \cdot \ldots \cdot (p-1) \cdot a = r_\alpha \cdot r_\beta \cdot r_\chi \cdot \ldots \cdot r_\lambda \text{ mod } p;$

$a \cdot 2a \cdot 3a \cdot \ldots \cdot (p-1) \cdot a = 1 \cdot 2 \cdot 3 \cdot \ldots (p-1) \text{ mod } p;$

$a^{p-1} \cdot (p-1)! = (p-1)! \text{ mod } p;$ Due to $(p-1)!$ and p are relatively prime $((p-1)!, p)=1$, then

$$a^{p-1}=1 \textbf{ mod } p \ \#$$

3. Mathematical Backgrounds

3.5. Number Theory

Euler's Function ψ(n) for $n \geq 1$ is the number of integers lees than n and relatively prime with n. $\psi(1)=0,\ \psi(2)=1,\ \psi(3)=2,\ \psi(4)=2,\ \psi(5)=4,\ \psi(6)=2,\ \psi(7)=6,\ \psi(8)=4,\ \psi(9)=6,\ \psi(10)=4,\ \psi(11)=10, \ldots$. If n is a prime number p, then $\psi(p)=p-1$.

Theorem 3.5.10. If $n=pq$, where p and q are the prime numbers, then $\psi(n)= =\psi(p)\psi(q)=(p-1)(q-1)$.

Proof: Let consider the complete set of residues $\{0,1,2,\ldots,pq-1\}$ by *modulo* $n=pq$. All this residues are relatively prime with $n=pq$, except $(p-1)$ elements $\{q,2q,3q,\ldots,(p-1)q\}$, $(q-1)$ elements $\{p,2p,3p,\ldots,(q-1)p\}$, and 0. Thus, $\psi(pq)=pq-(p-1)-(q-1)-1=pq-p-q+1=(p-1)(q-1)$.#

Example 3.5.15. $\psi(10)=\psi(2\cdot5)=\psi(2)\cdot\psi(5)=1\cdot4=4$.

Theorem 3.5.11. If p is a prime number, and $k>0$ integer number, then

$\psi(p)=p^k-p^{k-1}=p^{k-1}(p-1)$.

Proof: The set of integers which are less than p^k and are not relatively prime with p^k, includes the numbers $\{p,2p,3p,\ldots,(p^{k-1}-1)p\}$. It means that among p^k-1 numbers less than p^k there are $p^{k-1}-1$ integers are not relatively prime with p^k. Thus, $\psi(p)=p^k-1-(p^{k-1}-1)= p^k-p^{k-1}$.#

Example 3.5.16. $\psi(8)=\psi(2^3)=2^3-2^2=8-4=4$.

Theorem 3.5.12. Function $\psi(n\cdot m)$ is multiplicative function $\psi(n\cdot m)= =\psi(n)\cdot\psi(m)$, when $(n,m)=1$.

When $a=p1^{\alpha 1}p2^{\alpha 2}\ldots pr^{\alpha r}$, then $\psi(a)=\psi(p1^{\alpha 1})\psi(p2^{\alpha 2})\ldots\psi(pr^{\alpha r})=(p1^{\alpha 1}-p1^{\alpha 1-1})(p2^{\alpha 2}-p2^{\alpha 2-1})\ldots(pr^{\alpha r}-pr^{\alpha r-1})=a(1-1/p1)(1-1/p2)\ldots(1-1/pr)$.

Example 3.5.17. $\psi(2700)=?\ 270=2^2 3^3 5^2$. $\psi(2700)=2700(1-1/2)(1-1/3)(1-1/5)=720$.

3. Mathematical Backgrounds

3.5. Number Theory

Euler's Theorem. If $n \geq 0$ is an positive integer number, and $(a,n)=1$, where a is an integer, then

$$a^{\psi(n)}=1 \textbf{ mod } n.$$

Proof: let $\{r_1, r_2, r_3, \ldots, r_{\psi(n)}\}$ is a reduced residue system modulo n, then for $(a,n)=1$ numbers ar_1, ar_2, $ar_3, \ldots,$ $ar_{\psi(n)}$ will organize the same reduced residue system, such a way that

$ar_1 = r_\alpha mod\ n;$ $ar_2 = r_\beta mod\ n;$ $ar_3 = r_\chi mod\ n, \ldots, ar_{\psi(n)} = r_\lambda mod\ p,$

where $\{r_\alpha, r_\beta, r_\chi, \ldots, r_\lambda\}$ is a permutation of residues $\{r_1, r_2, r_3, \ldots, r_{\psi(n)}\}$.

Multiplying the right and left part of the last congruence we will get:

$a^{\psi(n)}\ r_1 \cdot r_2 \cdot r_3 \cdot \ldots \cdot r_{\psi(n)} = r_\alpha \cdot r_\beta \cdot r_\chi \cdot \ldots \cdot r_{\psi(n)}\ mod\ n;$

Taking into account, that $\{r_1, r_2, r_3, \ldots, r_{\psi(n)}, m)=1,$ then

$$a^{\psi(n)} = 1 \textbf{ mod } n.\#$$

Example 3.5.18. $3^{10}\ mod\ 11=?$. According to the Fermat's theorem $3^{10} = 1\ mod\ 11$, where $p=11$, and $a=3$.

Example 3.5.19. $3^{12}\ mod\ 26=?$. According to the Euler's theorem $3^{12}\ mod\ 26=1,$ where $n=26$, $\psi(26)=\psi(2 \cdot 13)=\psi(2) \cdot \psi(13)=1 \cdot 12=12.$

3. Mathematical Backgrounds

3.5. Number Theory

Liner Congruencies

The linear congruence is

$$ax=b \textbf{ mod } n,\ b<n.$$

There are three possibilities for the linear congruence solution x, namely, no solutions, one solution and a set of solutions satisfying this linear congruence.

Theorem 3.5.12. If $(a,n)=d$ is not a divider of b, then there are not solutions of linear congruence $ax=b$ **mod** n.

Proof: Suppose there is a solution x_0, that satisfy the linear congruence $ax_0=b$ **mod** n. According to the condition of the theorem d is a divider of a and n, what means that d have to be a divider of ax_0 and nq, as well as a divider of $ax_0-nq=b$. This implies a contradiction.#

Example 3.5.20. Linear congruence $2x=1 \ mod\ 4$ does not have a solution.

Theorem 3.5.13. If $(a,n)=1$ there is one solution of linear congruence $ax=b$ **mod** n.

Proof: Let's take a complete residue system $\{0,1,2,\dots,n-1\}$ by modulo n. Due to the fact that a and n are relatively prime the integer numbers $\{0\cdot a, 1\cdot a, 2\cdot a,\dots, (n-1)\cdot a\}$ create the complete residue system modulo n. Among all integer numbers there is one ax_0 and only one with residue equals to b.#

Example 3.5.21. Linear congruence $2x=1 \ mod\ 3$ has a solution $x_0=2$.

Computing Inverses a^{-1}

For $b=1$ linear congruence is $ax=1$ ***mod*** n, where $x=a^{-1}$, then $aa^{-1}=1$ ***mod*** n.

Let take two congruence $ax=1$ ***mod*** n and $1=a^{\psi(n)}$ ***mod*** n *(Euler's theorem)*, then multiply left and right part of this relations. As the result we will get:

$$ax=a^{\psi(n)} \textbf{ mod } n \Rightarrow x=a^{\psi(n)-1} \textbf{ mod } n,$$

$$\text{for prime } n \Rightarrow x=a^{n-2} \textbf{ mod } n.$$

Example 3.5.22. Find a solution of linear congruence $3x=1$ *mod* 7. 7 is prime number, then $x=a^{n-2}$ ***mod*** $n=3^{7-2}$ ***mod*** $7=3^5$ ***mod*** $7=5$.

Example 3.5.23. Find a solution of linear congruence $4x=1$ *mod* 9. $\psi(9)=6$, then $x=a^{\psi(n)-1}$ ***mod*** $n=4^{6-1}$ ***mod*** $9=4^5$ ***mod*** $9=7$.

Similar for case of computing inverse it have been shown that

3. Mathematical Backgrounds

3.5. Number Theory

Euclid's algorithm extended to Computing Inverses a^{-1}

```
begin "Return x such that ax mod n=1, where 0<a<n"
        g0:=n; g1:=a;
        u0:=1; v0:=0;
        u1:=0; v1:=1;
        while gi≠0 do "gi= uin+ via"
                begin
                        y:=gi-1 div gi;
                        gi+1= gi-1 –y* gi;
                        ui+1= ui-1 –y* ui;
                        vi+1= vi-1 –y* vi;
                        i:=i+1
                end;
        x:= vi-1;
        if x≥0 then a-1:=x else a-1:=x+n
```

3. Mathematical Backgrounds

3.5. Number Theory

Euclid's algorithm extended to Computing Inverses a^{-1}

The algorithm computes (a,n) by computing $g_{i+1}= g_{i-1}$ **mod** g_i for $i=1,2,\ldots$ until $g_i=0$, where $g_0 = n$, $g_1 = a$, and "$g_i= u_i n+v_i a$" is the loop invariant. When $g_i=0$, $g_{i-1} = (a,n)$. If $(a,n)=1$, then $g_{i-1}=1$ and $v_{i-1}a -1= u_{i-1}n$, giving $v_{i-1}a =1$ **mod** n. Thus, $x= v_{i-1}$ is an inverse of a **mod** n. Now x will be in the range $-n<x<n$. If x is negative, $x+n$ gives the solution in the range $0<x<n$.

The following illustrates the execution of the algorithm to solve the equation $3x$ mod $7 =1$.

i	g_i	u_i	v_i	y
0	7	1	0	
1	3	0	1	2
2	1	1	-2	3
3	0			

Because $v_2= -2$ is negative, the solution is $x=-2+7=5$.

Solution ax=b mod n, b<n; for the case (a,n)=1.

$x=ba^{\psi(n)-1}$ **mod** n,

for prime $n \Rightarrow x=ba^{n-2}$ **mod** n.

Example 3.5.24. Linear congruence $3x=3$ *mod* 7. Taking into account that $(3,7)=1$ and 7 is a prime number $x=ba^{n-2}$ **mod** $n=33^{7-2}$ **mod** $7=3^5$ **mod** $7=5$.

3. Mathematical Backgrounds

3.5. Number Theory

Theorem 3.5.14. If $(a,n)=d$, and $d \mid b$, then there are d solutions of linear congruence $ax=b$ **mod** n.

Proof: According to the condition of the theorem d is a divider of a, n and b. Then from congruence $ax=b$ **mod** n we can get $a_1dx=b_1d$ **mod** n_1d, or what the same the congruence $a_1x=b_1$ **mod** n_1, where $(a_1,n_1)=1$. The last congruence $a_1x=b_1$ **mod** n_1, has one solution x_0. Integers of the same class by modulo n/d will be the solutions for the congruence $ax=b$ **mod** n. Namely,

$$x_1=x_0 \textbf{ mod } n,$$

$$x_2=x_0+n/d \textbf{ mod } n,$$

$$x_3=x_0+2n/d \textbf{ mod } n,$$

$$\ldots,$$

$$x_d=x_0+(d-1)n/d \textbf{ mod } n.\#$$

Example 3.5.25. Find the solutions for the following linear congruence

$$6x=4 \text{ mod } 10.$$

Taking into account that $(6,10)=2$ and 2 is a divider of 4, we will get the congruence $3x=2$ *mod* 5. Then the solution of the last congruence is number $x_0=ba^{n-2}$ **mod** $n=23^{5-2}$ **mod** $5=23^3$ **mod** $5=4$.

$$x_1=x_0 \textbf{ mod } n=4 \textbf{ mod } 10=4;$$

$$x_2=x_0+n/d \textbf{ mod } n=4+10/2 \textbf{ mod } 10=9.$$

3. Mathematical Backgrounds

3.5. Number Theory

Testing of Primality

Several methods can be used to test a randomly selected number for primality. However, the most straightforward approaches are not computationally feasible. For example, a test could be based on next theorem, which states.

Theorem 3.5.15. If p is odd prime number, then the equation

$$x^2=1 \ \mathbf{mod}\ p$$

has only two solutions, namely $x=1$ and $x=-1$.

Proof: Really from $x^2=1\ \mathbf{mod}\ p$, we'll get $x^2-1=0\ \mathbf{mod}\ p$ and $(x-1)(x+1)=0\ \mathbf{mod}\ p$. According to the last equation the p should be a divider of $(x+1)$ or divider of $(x-1)$ or both $(x-1)$ and $(x+1)$. Let p is a divider of both $(x-1)$ and $(x+1)$, then $(x+1)=kp$ and $(x-1)=jp$ for integer numbers k and j. After subtraction the second equation from the first we will get $2=(k-j)p$ which is hold true only for $p=2$. It means that for any solution x, $p|(x+1)$ or $p|(x-1)$.

The last theorem can be formulated as: If equation $x^2=1\ \mathbf{mod}\ p$ has the solution differ than ± 1, then p is not a prime number.

Example 3.5.26. $x^2=1\ \mathbf{mod}\ 7$.

$1^2=1\ \mathbf{mod}\ 7;\ 2^2=4\ \mathbf{mod}\ 7;\ 3^2=2\ \mathbf{mod}\ 7;\ 4^2=2\ \mathbf{mod}\ 7;\ 5^2=4\ \mathbf{mod}\ 7;\ 6^2=1\ \mathbf{mod}\ 7;$

Solutions : $x=1;\ x=6 \bmod 7=-1.$

Example 3.5.27. $x^2=1\ \mathbf{mod}\ 7$.

$1^2=1\ \mathbf{mod}\ 8;\ 2^2=2\ \mathbf{mod}\ 8;\ 3^2=1\ \mathbf{mod}\ 8;\ 4^2=0\ \mathbf{mod}\ 8;\ 5^2=1\ \mathbf{mod}\ 8;\ 6^2=4\ \mathbf{mod}\ 8;\ 7^2=1\ \mathbf{mod}\ 8;$ ***Solutions :*** $x=1;\ x=3;\ x=5\ \mathbf{mod}\ 8=-3;\ x=7\ \mathbf{mod}\ 8=-1;$