Key Terms and Results

TERMS

a | *b* (*a* divides *b*) 整除: there is an integer *c* such that $b=ac$
a* and *b* are congruent modulo *m 模m同余: ***m* divides *a-b***
modular arithmetic 模算术: arithmetic done modulo an integer $m \geq 2$
prime 质数: an integer greater than 1 with exactly two positive integer divisors
composite 合数: an integer greater than 1 that is not prime
Mersenne prime 默森纳质数: a prime of the form $2^p - 1$, where p is prime
gcd(*a, b*) (greatest common divisor of *a* and *b*) 最大公约数: the largest integer that divides both a and b
relatively prime integers 互质: integers a and b such that $\gcd(a, b) = 1$
pairwise relatively prime integers 两两互质: a set of integers with the property that every pair of these integers is relatively prime
lcm(*a, b*) (least common multiple of *a* and *b*) 最小公倍数: the smallest positive integer that is divisible by both a and b
a* mod *b: the remainder when the integer a is divided by the positive integer b

***a*≡*b* (mod *m*) (*a* is congruent to *b* modulo *m*)**同余: $a - b$ is divisible by m

$n=(a_k a_{k-1} \ldots a_1 a_0)_b$: the base b representation of n
binary representation 二进制: the base 2 representation of an integer
octal representation 八进制: the base 8 representation of an integer
hexadecimal representation十六进制: the base 16 representation of an integer
linear combination of *a* and *b* with integer coefficients线性组合: an expression of the form $sa+tb$, where s and t are integers
Bézout coefficients of *a* and *b*贝祖系数: integers s and t such that the
Bézout identity 贝祖等式$sa + tb = \gcd(a, b)$ holds
inverse of a modulo m 逆: an integer ~a such that $\sim a a \equiv 1 \pmod{m}$
linear congruence 线性同余: a congruence of the form $ax \equiv b \pmod{m}$, where x is an integer variable
pseudoprime to the base *b* 伪质数: a composite integer n such that $b^{n-1} \equiv 1 \pmod{n}$
Carmichael number 卡迈克尔数: a composite integer n such that n is a pseudoprime to the base b for all positive integers b with $\gcd(b, n)=1$
primitive root of a prime *p*原始根: an integer r in $\mathbf{Z}_p$ such that every integer not divisible by p is congruent modulo p to a power of r
discrete logarithm of *a* to the base *r* modulo *p* 离散对数: the integer e with $0 \leq e \leq p-1$ such that $r^e \equiv a \pmod{p}$
encryption 加密: the process of making a message secret
decryption 解密: the process of returning a secret message to its original form
encryption key 加密密钥: a value that determines which of a family of encryption functions is to be used
shift cipher 移位密码: a cipher that encrypts the plaintext letter p as $(p+k)$ **mod** m for an integer k
affine cipher 仿法密码: a cipher that encrypts the plaintext letter p as $(ap+b)$ **mod** m for integers a and b with $\gcd(a, 26) = 1$
character cipher 字符密码: a cipher that encrypts characters one by one
block cipher 块密码: a cipher that encrypts blocks of characters of a fixed size

cryptanalysis 密码分析, 破译: the process of recovering the plaintext from ciphertext without knowledge of the encryption method, or with knowledge of the encryption method, but not the key

cryptosystem 密码系统: a five-tuple (P, C, K, E, D) where P is the set of plaintext messages, C is the set of ciphertext messages, K is the set of keys, E is the set of encryption functions, and D is the set of decryption functions
private key encryption 私钥加密: encryption where both encryption keys and decryption keys must be kept secret
public key encryption 公钥加密: encryption where encryption keys are public knowledge, but decryption keys are kept secret
RSA cryptosystem RSA 加密系统: the cryptosystem where $\boldsymbol{P}$ and $\boldsymbol{C}$ are both $\mathbf{Z}_{26}$, $\boldsymbol{K}$ is the set of pairs $k= (n, e)$ where $n= pq$ where p and q are large primes and e is a positive integer, $E_k(p)= p^e$ **mod** n, and $D_k(c) = c^d$ **mod** n where d is the inverse of e modulo $(p-1)(q-1)$
key exchange protocol 密钥交换协议: a protocol used for two parties to generate a shared key
digital signature 数字签名: a method that a recipient can use to determine that the purported sender of a message actually sent the message

RESULTS

division algorithm 除数算法: Let a and d be integers with d positive. Then there are unique integers q and r with $0 \leq r < d$

such that $a=dq + r$.

Let b be an integer greater than 1. Then if n is a positive integer, it can be expressed uniquely in the form $n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_1 b + a_0$.

The algorithm for finding the base b expansion of an integer (see Algorithm 1 in Section 4.2)

The conventional algorithms for addition and multiplication of integers (given in Section 4.2)

The modular exponentiation algorithm (see Algorithm 5 in Section 4.2)

Euclidean algorithm 欧几里得算法**:** for finding greatest common divisors by successively using the division algorithm (see Algorithm 1 in Section 4.3)

Bézout's theorem贝祖定理**:** If a and b are positive integers, then gcd(a, b) is a linear combination of a and b.

sieve of Eratosthenes 埃拉托斯特尼筛法**:** A procedure for finding all primes not exceeding a specified number n, described in Section 4.3

fundamental theorem of arithmetic 算术基本定理**:** Every positive integer can be written uniquely as the product of primes, where the prime factors are written in order of increasing size.

If a and b are positive integers, then ab = gcd(a, b) lcm(a, b).

If m is a positive integer and gcd(a, m) =1, then a has a unique inverse modulo m.

Chinese remainder theorem 中国余数定理**:** A system of linear congruences modulo pairwise relatively prime integers has a unique solution modulo the product of these moduli.

Fermat's little theorem 费马小定理**:** If p is prime and $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$.