MAT 258
Discrete Mathematics
Number Theory

Kenneth H. Rosen and Kamala Krithivasan

Discrete Mathematics 7E Global Edition Chapter 4

Fall 2018 Week 3

Introduction

If $a, b \in \mathbb{Z}$, with $a \neq 0$, a **divides** b ($a \mid b$) if there is $c \in \mathbb{Z}$ such that $b = ac$ or if $\frac{b}{a} \in \mathbb{Z}$. a is a **factor** or **divisor** of b, and b is a **multiple** of a. If a does not divide b, $a \nmid b$: $3 \nmid 7$ and $3 \mid 12$.
Let $n, d \in \mathbb{Z}$. How many positive integers not exceeding n are divisible by d?
There are $\lfloor n/d \rfloor$ positive multiples of d not exceeding n.
Let $a, b, c \in \mathbb{Z}$, $a \neq 0$. Then, if $a \mid b$,

- if $a \mid c$, then $a \mid b + c$
- then $a \mid bc$
- if $b \mid c$, then $a \mid c$
- if $a \mid c$, then $a \mid (mb + nc)$, where $m, n \in \mathbb{Z}$

Algorithm

Let $a \in \mathbb{Z}$ and $d \in \mathbb{Z}^+$. Then there are unique $q, r \in \mathbb{Z}$, with $0 \leq r < d$, such that $a = dq + r$. d is the **divisor**, a is the **dividend**, $q = a$ **div** $d = \lfloor a/d \rfloor$ is the **quotient** and $r = a$ **mod** $d = a - (a$ **div** $d)d$ is the **remainder**.

What are the quotient and remainder when 101 is divided by 11?

$101 = 11 \cdot 9 + 2$, so $9 = 101$ **div** 11 and $2 = 101$ **mod** 11.

What are the quotient and remainder when -11 is divided by 3?

$-11 = 3(-4) + 1$, so $-4 = -11$ **div** 3 and $1 = -11$ **mod** 3.

Programming languages may have operators for modular arithmetic, but may return $-d < a - \lceil a/d \rceil d \leq 0$ as the remainder when $a < 0$, and may return values when $d \leq 0$.

Definitions

If $a, b \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$, then a **is congruent to** b **modulo** m ($a \equiv b \pmod{m}$) if $m \mid (a-b)$, a **congruence** whose **modulus** is m. If $m \nmid (a-b)$, then $a \not\equiv b \pmod{m}$. $a \equiv b \pmod{m}$ if and only if $a \bmod m = b \bmod m$.

$17 \equiv 5 \pmod{6}$, since $6 \mid (17-5)$, and $24 \not\equiv 14 \pmod{6}$, since $6 \nmid (24-14)$.

$a \equiv b \pmod{m}$ if and only if there is $k \in \mathbb{Z}$ such that $a = b + km$. All integers congruent to an integer a modulo m is the **congruence** or **equivalence class of** a **modulo** m. In Chapter 9, it will be seen that there are m pairwise disjoint equivalence classes modulo m whose union is $\mathbb{Z}$.

If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a + c \equiv b + d \pmod{m}$ and $ac \equiv bd \pmod{m}$.

Arithmetic

$\mathbb{Z}_m = \{0, \ldots, m-1\} \subset \mathbb{Z}$ has arithmetic operations $+_m$ and $\cdot_m$:

$$a +_m b = (a + b) \textbf{ mod } m = [(a \textbf{ mod } m) + (b \textbf{ mod } m)] \textbf{ mod } m$$

$$a \cdot_m b = ab \textbf{ mod } m = (a \textbf{ mod } m)(b \textbf{ mod } m) \textbf{ mod } m$$

$7 +_{11} 9 = 5$ and $7 \cdot_{11} 9 = 8$

The operations satisfy these properties: if $a, b, c \in \mathbb{Z}_m$,

- **Closure**: $a +_m b \in \mathbb{Z}_m$, and $a \cdot_m b \in \mathbb{Z}_m$
- **Associativity**: $(a +_m b) +_m c = a +_m (b +_m c)$, and $(a \cdot_m b) \cdot_m c = a \cdot_m (b \cdot_m c)$
- **Commutativity**: $a +_m b = b +_m a$, and $a \cdot_m b = b \cdot_m a$
- **Identity elements**: $0 \in \mathbb{Z}_m$, where $a +_m 0 = 0 +_m = a$, $1 \in \mathbb{Z}_m$, $(m > 1)$, where $a \cdot_m 1 = 1 \cdot_m a = a$
- **Additive inverse**: $0 +_m 0 = 0$ and $a +_m (m - a) = 0$ when $a > 0$, $m - a \in \mathbb{Z}_m$. a may have no multiplicative inverse.
- **Distributivity**: $a \cdot_m (b +_m c) = (a \cdot_m b) +_m (a \cdot_m c)$ and $(a +_m b) \cdot_m c = (a \cdot_m c) +_m (b \cdot_m c)$

Primes

$p \in \mathbb{Z}$, $p > 1$ is **prime** if the only positive factors of p are 1 and p, otherwise p is **composite**. n is composite if and only if there is $a \in \mathbb{Z}$ such that $a \mid n$ and $1 < a < n$.

7 is prime, 9 is composite, since $3 \mid 9$.

The Fundamental Theorem of Arithmetic

> *Every integer greater than 1 can be written uniquely as a prime or as the product of two or more primes where the prime factors are written in nondecreasing order.*

$100 = 2 \cdot 2 \cdot 5 \cdot 5 = 2^2 \cdot 5^2$, $641 = 641$, $999 = 3 \cdot 3 \cdot 3 \cdot 37 = 3^3 \cdot 37$,
$1024 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2^{10}$

Trial Division

If $n \in \mathbb{Z}$ is composite, then n has a prime divisor less than or equal to $\sqrt{n}$. This leads to the brute-force algorithm for checking primality called **trial division**: 101 is prime, since it is not divisible by $2, 3, 5, 7 < \sqrt{101}$.
Trial division can be used in determining prime factorization: $7007 \neq 2 \cdot n \neq 3 \cdot n \neq 5 \cdot n = 7 \cdot 1001 = 7^2 \cdot 143 \neq 7^3 \cdot n = 7^2 \cdot 11 \cdot 13$.

Sieve of Eratosthenes

The **Sieve of Eratosthenes** is used to determine all primes not exceeding a specified positive integer. **Multiples of: 2, 3, 5, 7.**

1	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	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Distribution

There are an infinite number of primes, proven by Euclid.
Primes of the form $2^p - 1$, p prime, are **Mersenne primes**: largest known is $p = 77232917$, 26 December 2017, efficiently tested using the Lucas-Lehmer test.
Prime Number Theorem: The ratio of the number of primes not exceeding x and $\dfrac{x}{\ln x}$ approaches 1 as $x \to \infty$.
Cunningham numbers $k^n \pm 1$, where $k, n \in \mathbb{Z}$, $k \ll n$, are targets of communal factorization efforts.
Every arithmetic progression $ak + b$, a, b relatively prime, $k = 1, 2, \ldots$, has an infinite number of primes. For every $n \in \mathbb{Z}^+$, there is an arithmetic progression $ak + b$, $k = 1, \ldots, n$ where each is prime.

Open Conjectures

Goldbach's Conjecture: Every even integer greater than 2 is the sum of two primes.

- Chen (1973): Every sufficiently large even integer is the sum of a prime and a prime or a product of two primes.
- Ramaré (1995): Every even integer greater than 2 is the sum of at most six primes.
- Helfgott (2013): Every even integer greater than 2 is the sum of at most four primes.

There are infinitely many primes of the form $n^2 + 1$, $n \in \mathbb{Z}$. Iwaniec (!973): there are infinitely many $n^2 + 1$ that are prime or the product of at most two primes.

Twin Prime Conjecture: There are infinitely many pairs $n, n + 2 \in \mathbb{Z}$ that are both prime.

- Zhang (2013): There are infinitely many pairs $n, n + N \in \mathbb{Z}$ that are both prime, $N < 7 \times 10^7$.

Greatest Common Divisor

The largest $d \in \mathbb{Z}$ such that $d \mid a$, $d \mid b$, $a, b \in \mathbb{Z}$, $a \neq 0$ or $b \neq 0$, is the **greatest common divisor** of a and b, $\gcd(a, b) = d$.
$\gcd(24, 36) = 12$, $\gcd(17, 22) = 1$.
a and b are **relatively prime** if $\gcd(a, b) = 1$. $a_1, a_2, \ldots, a_n$ are **pairwise relatively prime** if $\gcd(a_i, a_j) = 1$ whenever $1 \leq i < j \leq n$.
10, 17, 21 are pairwise relatively prime, 10, 19, 24 are not pairwise relatively prime, since $\gcd(10, 24) = 2$.
If $a = \prod_{i=1}^{n} p_i^{a_i}$ and $b = \prod_{i=1}^{n} p_i^{b_i}$, $a_i, b_i \geq 0$, are prime factorizations, then $\gcd(a, b) = \prod_{i=1}^{n} p_i^{\min(a_i, b_i)}$.
Since $120 = 2^3 \cdot 3 \cdot 5$ and $500 = 2^2 \cdot 5^3$, $\gcd(120, 500) = 2^2 \cdot 3^0 \cdot 5^1 = 20$.

Least Common Multiple

The **least common multiple** of $a, b \in \mathbb{Z}^+$ is the smallest positive integer divisible by both a and b, $\text{lcm}(a, b)$. If $a = \prod_{i=1}^{n} p_i^{a_i}$ and $b = \prod_{i=1}^{n} p_i^{b_i}$, $a_i, b_i \geq 0$, are prime factorizations, then

$$\text{lcm}(a, b) = \prod_{i=1}^{n} p_i^{\max(a_i, b_i)}.$$

$\text{lcm}(2^3 3^5 7^2, 2^4 3^3) = 2^4 3^5 7^2$.

If $a, b \in \mathbb{Z}^+$, $ab = \gcd(a, b) \cdot \text{lcm}(a, b)$.

Euclidean Algorithm

Let $a = bq + r$, where $a, b, q, r \in \mathbb{Z}$. Then $\gcd(a, b) = \gcd(b, r)$.
By repeatedly applying the division algorithm, if $a = r_0$, $b = r_1$:
$r_i = q_i r_{i+1} + r_{i+2}$, where $0 \leq r_{i+2} < r_{i+1}$,
$\gcd(a, b) = \gcd(r_i, r_{i+1}) = \gcd(r_n, 0) = r_n$.
To find $\gcd(414, 662)$: $662 = 414 \cdot 1 + 248$, $414 = 248 \cdot 1 + 166$,
$248 = 166 \cdot 1 + 82$, $166 = 82 \cdot 2 + 2$, $82 = 2 \cdot 41$. Thus,
$\gcd(414, 662) = 2$.
`gcd`(a, b) where $b < a$, $a, b \in \mathbb{Z}^+$

- `while` $b > 0$
  - $a \leftarrow b + (a \textbf{ mod } b)$
  - $b \leftarrow a - b$
  - $a \leftarrow a - b$
- `return` a

Bézout's Theorem

Bézout's Identity: If $a, b \in \mathbb{Z}^+$, there exist $s, t \in \mathbb{Z}$ such that $\gcd(a, b) = sa + tb$, where s and t are the **Bézout coefficients** of a and b.
$252 = 198 \cdot 1 + 54$, $198 = 54 \cdot 3 + 36$, $54 = 36 \cdot 1 + 18$, $36 = 18 \cdot 2$:

$$\gcd(252, 198) = 18 = 54 - 36 = 54 \cdot 4 - 198 = 252 \cdot 4 - 198 \cdot 5.$$

If $a, b, c \in \mathbb{Z}^+$ such that $\gcd(a, b) = 1$ and $a \mid bc$, then $a \mid c$.
If p is prime, $p \mid \prod_{i=1}^{n} a_i$, where $a_i \in \mathbb{Z}$, then $p \mid a_i$ for some i, $1 \leq i \leq n$.
Let $m \in \mathbb{Z}^+$, $a, b, c \in \mathbb{Z}$. If $ac \equiv bc \pmod{m}$ and $\gcd(c, m) = 1$, then $a \equiv b \pmod{m}$.

Solving Linear Congruences

When $m \in \mathbb{Z}^+$ and $a, b \in \mathbb{Z}$, $ax \equiv b \pmod{m}$ is a **linear congruence**. How can we find all $x \in \mathbb{Z}$ that satisfy this congruence?

$\bar{a} \in \mathbb{Z}$ is an **integer of a modulo m** if $a\bar{a} \equiv 1 \pmod{m}$. If $\gcd(a, m) = 1$, $\bar{a}$ exists and is unique. $7 = 2 \cdot 3 + 1$, so $1 = 1 \cdot 7 - 2 \cdot 3$, so $-2 \equiv 5 \pmod{7}$ is an inverse of 3 modulo 7.

$4620 = 45 \cdot 101 + 75$, $101 = 1 \cdot 75 + 26$, $75 = 2 \cdot 26 + 23$, $26 = 1 \cdot 23 + 3$, $23 = 7 \cdot 3 + 2$, $3 = 1 \cdot 2 + 1$, so

$$\begin{aligned} 1 &= 3 - 2 = 8 \cdot 3 - 23 = 8 \cdot 26 - 9 \cdot 23 = 26 \cdot 26 - 9 \cdot 75 \\ &= 26 \cdot 101 - 35 \cdot 75 = 1601 \cdot 101 - 35 \cdot 4620 \end{aligned}$$

Thus, $1 \equiv (-35) \cdot 4620 = 66 \cdot 4620 \pmod{101}$ and $1 \equiv 1601 \cdot 101 \pmod{4620}$.

Since 5 is the inverse of 3 modulo 7, $3x \equiv 4 \pmod{7}$ can be solved by multiplying both sides by 5:

$5(3x) = (5 \cdot 3)x \equiv x \equiv 5 \cdot 4 = 20 \equiv 6 \pmod{7}$.

Chinese Remainder Theorem

Let $m_1, m_2, \ldots, m_n \in \mathbb{Z}^+$ be pairwise relatively prime and greater than one, and $a_1, a_2 \ldots, a_n \in \mathbb{Z}$. Then the system $x \equiv a_i \pmod{m_i}$, $1 \leq i \leq n$ has a unique solution modulo $m = m_1 m_2 \cdots m_n$.

Let $M_k = m/m_k$, then $\gcd(M_k, m_k) = 1$ and there exists $y_k \in \mathbb{Z}$ such that $M_k y_k \equiv 1 \pmod{m_k}$. Thus, $x = \sum_{i=1}^{n} a_i M_i y_i$.

Let $x \equiv 2 \pmod 3$, $x \equiv 3 \pmod 5$ and $x \equiv 2 \pmod 7$. Then $M = 105$, $35 \cdot 2 \equiv 1 \pmod 3$, $21 \cdot 1 \equiv 1 \pmod 5$, and $15 \cdot 1 \equiv 1 \pmod 7$.Then,

$$x \equiv 35{\cdot}2{\cdot}2{+}21{\cdot}1{\cdot}3{+}15{\cdot}1{\cdot}2 = 140{+}63{+}30 = 233 \equiv 23 \pmod{105}.$$

If $x \equiv 1 \pmod 5$, $x \equiv 2 \pmod 6$ and $x \equiv 3 \pmod 7$, $x = 5t + 1 \equiv 2 \pmod 6$, $t \in \mathbb{Z}$, $t \equiv 5 \pmod 6$, thus $t = 6u + 5$ and $x = 30u + 26 \equiv 3 \pmod 7$, $u \in \mathbb{Z}$, $u \equiv 6 \pmod 7$. Thus $u = 7v + 6$, $v \in \mathbb{Z}$ and $x = 210v + 206$, so $x \equiv 206 \pmod{210}$.

Arithmetic of Large Numbers

By the Chinese Remainder Theorem, each integer $0 \leq n < 12$ can be uniquely represented by an ordered pair $(n \bmod 3, n \bmod 4)$. Arithmetic (modulo 12) can be performed by componentwise arithmetic (modulo 3 and 4, respectively) on the pair.

Integers $0 \leq n < 89403930 = 99 \cdot 98 \cdot 97 \cdot 95$ can be represented by ordered 4-tuples $(n \bmod 99, n \bmod 98, n \bmod 97, n \bmod 95)$: 123684 can be represented by $(33, 8, 9, 89)$, 413456 can be represented by $(32, 92, 42, 16)$. $123684 + 413456$ is represented by $(65, 2, 51, 10)$ which represents 537140.

$\gcd(2^a - 1, 2^b - 1) = 2^{\gcd(a,b)} - 1$ allows an easy way to find large relatively prime numbers to use as moduli for tuple representation of large numbers.

Fermat's Little Theorem and Pseudoprimes

If p is prime, and $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$. For $a \in \mathbb{Z}$, $a^p \equiv a \pmod{p}$.
7^{222} **mod** $11 \equiv (7^{10})^{22}7^2 \equiv 49 \equiv 5 \pmod{11}$.
Composite integers n such that $b^{n-1} \equiv 1 \pmod{n}$ are **pseudoprimes to the base** b. Among the positive integers less than 10^{10}, there are 455052512 primes, but only 14884 pseudoprimes to the base 2. A composite number n that satisfies $b^{n-1} \equiv 1 \pmod{n}$ for all $b \in \mathbb{Z}^+$ with $\gcd(b, n) = 1$ is a **Carmichael number**. 561 is a Carmichael number.

Primitive Roots and Discrete Logarithms

If p is prime, and $r \in \mathbb{Z}_p$ $(0 \leq r < p)$, if every nonzero element of $\mathbb{Z}_p$ is a power of r, r is a **primitive root modulo** p.
$2, 4, 8, 16 \textbf{ mod } 11 = 5, 10, 20 \textbf{ mod } 11 = 9, 18 \textbf{ mod } 11 = 7, 14 \textbf{ mod } 11 = 3, 6, 12 \textbf{ mod } 11 = 1$ are the powers of $2 \in \mathbb{Z}_{11}$, so 2 is primitive root modulo 11.
$3, 9, 27 \textbf{ mod } 11 = 5, 15 \textbf{ mod } 11 = 4, 12 \textbf{ mod } 11 = 1$ are the powers of $3 \in \mathbb{Z}_{11}$, so 3 is not a primitive root modulo 11. For every prime p, there is a primitive root modulo p.
If p is prime, r is a primitive root modulo p and $a = r^e \textbf{ mod } p$, then e is the **discrete logarithm of** a **modulo** p **to the base** r, $\log_r a = e$ (where the prime p is understood). When $p = 11$, $\log_2 3 = 8$ and $\log_2 5 = 4$.

Caesar Cipher

Replace letters of the English alphabet with numbers in $\mathbb{Z}_{26}$: $\texttt{A} \mapsto 0$, $\texttt{B} \mapsto 1$, $\ldots$, $\texttt{Z} \mapsto 25$. Caesar's **encryption** method can be represented by a function $f_p(x) : \mathbb{Z}_{26} \to \mathbb{Z}_{26}$, $f(x) = (x + p)$ **mod** 26, a **shift cipher**.
For a message "`MEET YOU IN THE PARK''`: replace letters with numbers,

12 4 4 19 24 14 20 8 13 19 7 4 15 0 17 10

then apply $f_3(x)$, back to letters: "`PHHW BRX LQ WKH SDUN`". To recover the original message by **decryption**, the inverse $f_p^{-1}(x) = (x - p)$ **mod** 26. p is called the **key**.
"`STOP GLOBAL WARMING`" shift encoded by key 11 is "`DEZA RWZMLW HLCXTYR`".
"`LEWLYPLUJL PZ H NYLHA ALHJOLY`" was shift encoded by key 7 from "`EXPERIENCE IS A GREAT TEACHER`".

Affine Ciphers and Cryptanalysis

Shift ciphers can be generalized to **affine ciphers** with an affine encryption function $f_{a,b}(x) = (ap + b)$ **mod** 26, where $\gcd(a, 26) = 1$.
`K` is affine encoded by $f_{7,3}(x)$ to `V`.
To decrypt a message encoded by an affine cipher using $f_{a,b}(x)$: consider $f_{a,b}(x) = c \equiv (ax + b) \pmod{26}$:

$$c - b \equiv ax \pmod{26} \Longrightarrow \bar{a}(c - b) \equiv x \pmod{26},$$

where $\bar{a}a \equiv 1 \pmod{26}$, thus $f^{-1}_{a,b}(x) = \bar{a}(x - b)$ **mod** 26.
Recovering plaintext from ciphertext without knowledge of the encryption method or the key is **cryptanalysis** or **code breaking**. For English messages encoded by shift cipher with an unknown key, use relative frequency of occurrence of letters: `E` 13%, `T` 9%, `A`, `O` both 8%, `I`, `N`, `S` all 7%, `H`, `R` 6%.
"`ZNK KGXRE HOXJ MKZY ZNK CUXS`" was shift encoded from "`THE EARLY BIRD GETS THE WORM`" with key 6 (`E` $\mapsto$ `K`).

Block Ciphers

Shift and affine ciphers are **character** or **monoalphabetic ciphers**, which are subject to cryptanalysis by frequency. Replacing blocks of letters with blocks of letters are **block ciphers**.

A **transposition cipher** splits a message into blocks of size m and rearranges the letters within the block, by a permutation $\sigma : \{1, 2, \ldots, m\} \to \{1, 2, \ldots, m\}$—decryption is done rearranging letters within the blocks by σ^{-1}.

With blocks of 4 letters, using the permutation σ, $\sigma(1) = 3$, $\sigma(2) = 1$, $\sigma(3) = 4$ and $\sigma(4) = 2$, "`PIRATE ATTACK`" is encrypted to "`IAPR ETTA AKTC`", and the encoded message "`SWUE TRAE OEHS`" is encrypted from "`USE WATER HOSE`".

Cryptosystems

A **cryptosystem** is a 5-tuple $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$, where $\mathcal{P}$ is the set of plaintext strings, $\mathcal{C}$ is the set if ciphertext strings, $\mathcal{K}$ is the **keyspace** of all possible keys, $\mathcal{E}$ is the set of encryption functions, and $\mathcal{D}$ is the set of decryption functions. Given a key $k \in \mathcal{K}$, let $E_k \in \mathcal{E}$ be the encryption function associated with the key, and $D_k = E_k^{-1} \in \mathcal{D}$ is the decryption function that decrypts ciphertext that was encrypted by E_k.
The shift cipher cryptosystem has $\mathcal{P} = \mathcal{C}$ is the set of strings with alphabet $\mathbb{Z}_{26}$, $\mathcal{K} = \mathbb{Z}_{26}$,
$\mathcal{E} = \{E_k(p) = c, c_i = (p_i + k) \textbf{ mod } 26, k \in \mathcal{K}\}$,
$\mathcal{E} = \{D_k(c) = p, p_i = (c_i - k) \textbf{ mod } 26, k \in \mathcal{K}\}$.

The RSA Cryptosystem

Private key cryptosystems are dependent on knowledge of a privately-held key for encryption, and thus decryption. Shift and affine ciphers, as classical ciphers, are all private-key cryptosystems. Modern private-key cryptosystems are much more sophisticated, such as those under the Advanced Encryption Standard, which requires secure communication keys to be used. New keys have to be generated per message and stored securely.

Public key cryptosystems everyone can have a publicly known encryption key, and only the decryption keys are kept secret, and only the intended recipient of a message can decrypt it, as knowledge of the encryption key does not let someone recover the plaintext without an extraordinary amount of work.

In the **RSA Cryptosystem**, each individual has an encryption key $(n = pq, e)$, where $n = pq$, p, q are large primes (maybe 200 digits each), and $\gcd(e, (p-1)(q-1)) = 1$.

RSA Encryption

Plaintext English message translate each letter to a two-digit number in $\mathbb{Z}_{26}$ as with shift ciphers, which are concatenated into strings of digits, which is divided into blocks of $2N$ digits, where the $2N$-digit number $2525\ldots25 \leq n$ (the last block may be padded with zeros at the end). Thus, the plaintext message M is represented by a sequence of integers $m_1, m_2, \ldots, m_k$.
$E_{(n,e)}(M) = C$ where $c_i = m_i^e \ \mathbf{mod}\ n$.
As an example, $(2537 = 43 \cdot 59, 13)$ is an encryption key, as $\gcd(13, 42 \cdot 58) = 1$. To encrypt `STOP`, the message is translate to the string 18191415, and the sequence $1819, 1415$.

$$1819^{13} = 1819^8 \cdot 1819^4 \cdot 1819 \equiv 1844 \cdot 1858 \cdot 1819 \equiv 2081 \pmod{2537}$$
$$1415^{13} = 1415^8 \cdot 1415^4 \cdot 1415 \equiv 1122 \cdot 1417 \cdot 1415 \equiv 2182 \pmod{2537}$$

The encrypted message is 2081 2182.

RSA Decryption

The decryption key d is such that $de \equiv 1 \pmod{(p-1)(q-1)}$, with decryption function $D_{(n,e)}(C) = M$ where $m_i = c_i^d$ **mod** n.
$c_i^d \equiv (m_i^e)^d = m_i^{1+k(p-1)(q-1)} \pmod{n}$. Assuming $\gcd(m_i, p) = \gcd(m_i, q) = 1$, Fermat's little theorem says

$$m_i^{p-1} \equiv 1 \pmod{p} \implies c_i^d \equiv m_i \cdot (m_i^{p-1})^{k(q-1)} \equiv m_i \pmod{p}$$
$$m_i^{q-1} \equiv 1 \pmod{q} \implies c_i^d \equiv m_i \cdot (m_i^{q-1})^{k(p-1)} \equiv m_i \pmod{q}$$

Since $\gcd(p, q) = 1$, by the Chinese remainder theorem, $c_i^d \equiv m_i \pmod{pq}$.
$(2537, 13)$ has a decryption key $d = 937$. A message 0981 0461 encrypted with this encryption key can be decrypted as follow: 981^{937} **mod** $2537 = 704$, 461^{937} **mod** $2537 = 1115.07041115$ translates to `HELP`.

RSA as Public Key Cryptosystem

To use RSA encryption:

- Generate large primes p, q
- p and q generate $n = pq$ and $(p-1)(q-1)$
- Generate e such that $\gcd(e, (p-1)(q-1)) = 1$
- e, p, and q determines the private key d, such that $de \equiv 1 \pmod{(p-1)(q-1)}$

Parties can send encrypted message m_i to a party with encryption key (n, e) by sending $c_i = m_i^e \textbf{ mod } n$, which only the recipient can decrypt back to $m_i c_i^d \textbf{ mod } n$.
Decryption through the public values n and e cannot be done without factoring n, which is believed to be a difficult problem.
Note that sophistication of computers often leads to larger values for p and q.

Cryptographic Protocols

The **Diffie-Hellman key agreement protocol** can be used to share a common key between two parties:

- Alice and Bob agree (publicly) to use a prime p and a primitive root a of p
- Alice has a private key k_1 and Bob has a private key k_2
- Alice (publicly) sends Bob a^{k_1} **mod** p to Bob, and Bob (publicly) sends a^{k_2} **mod** p to Alice
- Alice and Bob use the shared key $(a^{k_1})^{k_2}$ **mod** $p = (a^{k_2})^{k_1}$ **mod** p.

Usually p has 300 digits and k has 100 digits.
RSA can be used for **digital signatures**: a sender with encryption key (n, e) and decryption key d sends a "decrypted" message $c_i = m_i^d$ **mod** n, which can be "encrypted" to the original message $m_i = c_i^e$ **mod** n by any recipient who knows the sender's encryption key.