CHAPTER 2: CRYPTOGRAPHY AND NUMBER THEORY

NOTATION: $\mathbb{Z}_n = \{0,1,2,...,n-1\}$ (set of possible remainders when dividing any integer by n)

2.1 Cryptography and Modular Arithmetic

Introduction to Cryptography (study of methods for sending and receiving secret messages)

Sender $\underset{\text{Adversary}}{\rightarrow}$ Receiver

Private-Key Cryptography

Caesar cipher – cyclic shift of alphabet
- Plaintext (original message)
- Ciphertext (encrypted message)

Alphabet shifted 5 places to the left

0	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
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	0	1	2	3	4

Caesar cipher (A→F, B→G, C→H, …, Z→E)

Plaintext	R	O	W	A	N
Ciphertext	W	T	B	F	S

Euclid's Division Theorem: Let n be a positive integer. Then for every integer m, there exist unique integers q and r such that $m = nq + r$ with $0 \le r < n$.

Example:
(a) Let $n = 3$ and $m = 14$. Then $14 = 3 \cdot 4 + 2$ and so $q = 4$ and $r = 2$.
(b) Let $n = 7$ and $m = -16$. Then $-16 = 7 \cdot (-3) + 5$ and so $q = -3$ and $r = 5$.

Congruence Modulo *n*

Definition: Let l and m be integers and n a positive integer (called the modulus).
(a) We write m div n to mean the quotient q when m is divided by n, i.e. $q = m \text{ div } n$.
(b) We write $m \bmod n$ to mean the remainder $r \in \mathbb{Z}_n$ when m is divided by n, i.e. $r = m \bmod n$.
(c) We say that m and l are *congruent modulo n* and write $m \equiv l \bmod n$ if they have the same remainder when each is divided by n, or equivalently, n divides the difference $m - l$, i.e. $m - l = nq$ for some integer q.

NOTE: By Euclid's Division Theorem, $m \bmod n$ is well-defined and unique.

Example:
(a) 14 div $3 = 4$ (since $14 = 3 \cdot 4 + 2$) and -16 div $7 = -3$ (since $-16 = 7 \cdot (-3) + 5$).

(b) $14 \bmod 3 = 2$ (since $14 = 3 \cdot 4 + 2$) and $-16 \bmod 7 = 5$ (since $-16 = 7 \cdot (-3) + 5$)
(c) $26 \equiv 14 \bmod 3$ and $26 \equiv -16 \bmod 7$

NOTE: How do the answers for $16 \bmod 7$ and $-16 \bmod 7$ compare?

Caesar Cipher as Modular Congruence (same remainder): Let $a \in \mathbb{Z}$.

Encryption: A plaintext message M is encrypted using a Caesar cipher $C_a(x)$ with shift a by substituting each letter in M, specified by position x, with the letter having position

$$y = C_a(x) = (x + a) \bmod 26$$

Example: Given plaintext message ROWAN whose letters having positions $\{17,14,22,0,13\}$ in the alphabet, its Caesar cipher $C_5(x)$ (shift by 5) would be given by

$$C_5(17) = (17+5) \bmod 26 = 22 \quad (W)$$
$$C_5(14) = (14+5) \bmod 26 = 19 \quad (T)$$
$$C_5(22) = (22+5) \bmod 26 = 1 \quad (B)$$
$$C_5(0) = (0+5) \bmod 26 = 5 \quad (F)$$
$$C_5(14) = (13+5) \bmod 26 = 18 \quad (S)$$

This translates to the ciphertext WTBFS.

Decryption: A ciphertext message C, encrypted from a plaintext message M using a Caesar cipher $C_a(x)$ with shift a, can be decrypted using the inverse Caesar cipher $C_{-a}(y)$, by substituting each letter in C, specified by position y, with the letter having position

$$x = C_{-a}(y) = (y - a) \bmod 26$$

Example: Given ciphertext message WTBFS whose letters having positions $\{22,19,1,5,18\}$ and obtained from the Caesar cipher $C_5(x)$, we can decrypt it as follows using the inverse $C_{-5}(y)$:

$$C_{-5}(22) = (22-5) \bmod 26 = 17 \quad (R)$$
$$C_{-5}(19) = (19-5) \bmod 26 = 14 \quad (O)$$
$$C_{-5}(1) = (1-5) \bmod 26 = -4 \bmod 26 = 22 \quad (W)$$
$$C_{-5}(5) = (5-5) \bmod 26 = 0 \quad (A)$$
$$C_{-5}(18) = (18-5) \bmod 26 = 13 \quad (N)$$

This translates to the plaintext message ROWAN.

NOTE: It is necessary for the receiver to know the shift a (also called the *key* and kept secret) in order to decrypt messages using a Caesar cipher.

Public-Key Cryptography: ~~Alice~~ (sender) sends message M to ~~Bob~~ (receiver):

Public key P
Secret key S

Encryption: If Bob wants to send Alice a message M, he performs the following:

1. Bob obtains Alice's public key P_A
2. Bob applies Alice's public key to plaintext M to create ciphertext $C = P_A(M)$.

Decryption: If Alice wants to read Bob's message M, she performs the following:

1. Alice obtains Bob's ciphertext $C = P_A(M)$.
2. Alice applies her secret key S_A to ciphertext C to decrypt it and obtain plaintext $M = S_A(C) = S_A(P_A(M))$

NOTE: Similarly, if Alice wants to reply to Bob, then she uses Bob's public key P_B to encrypt her message, which Bob will be able to decrypt using his secret key S_B.

Arithmetic Modulo n

Motivating Examples:

(a) $(21+38) \bmod 9 = (21 \bmod 9) + (38 \bmod 9)$

(b) $(21+35) \bmod 9 \stackrel{?}{=} (21 \bmod 9) + (35 \bmod 9)$

(c) $12 \cdot 20 \bmod 9 \stackrel{?}{=} (12 \bmod 9)(20 \bmod 9)$

(d) $12 \cdot 40 \bmod 9 \stackrel{?}{=} (12 \bmod 9)(40 \bmod 9)$

Lemma:

(a) $(i+j) \bmod n = (i \bmod n + j \bmod n) \bmod n$

(b) $(i \cdot j) \bmod n = (i \bmod n) \cdot (j \bmod n) \bmod n$

Shorthand Notation: $i +_n j = (i+j) \bmod n$, $i \cdot_n j = (i \cdot j) \bmod n$

Fact: Modular arithmetic satisfies all the usual properties of arithmetic (commutative, associative, and distributive laws).

Cryptography Using Addition mod n

We already saw an example of cryptography using modular addition, namely the Caesar cipher (addition modulo 26). In general, we can encrypt using any modulus n. However, there are shortfalls to using a modulus $n \neq 26$.

Encryption: The encryption of a plaintext message M using *addition* by a mod n is given by the ciphertext message

$$P(M) = M +_n a$$

where each letter x of M is mapped to the letter $P(x) = x +_n a$.

Example: Let M = ROWAN whose letters have positions {17,14,22,0,13}. Then using encryption of addition by 20 mod 13 yields

$$P(17) = 17 +_{13} 20 = 11 \quad (L)$$
$$P(14) = 14 +_{13} 20 = 8 \quad (I)$$
$$P(22) = 22 +_{13} 20 = 3 \quad (D)$$
$$P(0) = 0 +_{13} 20 = 7 \quad (H)$$
$$P(13) = 13 +_{13} 20 = 7 \quad (H)$$

This yields the ciphertext message $P(M)$ = LIDHH. Observe that the cipher $P(x) = x +_{13} 20$ is a two-to-one function since

$P(0) = P(13) = 7$ $\quad$ $P(6) = P(19) = 0$
$P(1) = P(14) = 8$ $\quad$ $P(7) = P(20) = 1$
... $\quad$ ...
$P(5) = P(18) = 12$ $\quad$ $P(12) = P(25) = 6$

Thus, it is impossible to uniquely decrypt messages when $n < 26$ using the inverse cipher, addition by –20 mod 13, since it is impossible to obtain the letter R, O, W, N (those beyond position 12).

Cryptography Using Multiplication mod n

Encryption: The encryption of a plaintext message M using *multiplication* by a mod n is given by the ciphertext message

$$P(M) = M \cdot_n a$$

where each letter x of M is mapped to the letter $P(x) = x \cdot_n a$.

Example: Let M=ROWAN whose letters have positions {17,14,22,0,13}.
(a) Then using encryption of multiplication by 5 mod 26, i.e. $P(x) = x \cdot_{26} 5$ yields

$$P(17) = 17 \cdot_{26} 5 = 7 \quad (H)$$
$$P(14) = 14 \cdot_{26} 5 = 18 \quad (S)$$
$$P(22) = 22 \cdot_{26} 5 = 6 \quad (G)$$
$$P(0) = 0 \cdot_{26} 5 = 0 \quad (A)$$
$$P(13) = 13 \cdot_{26} 5 = 13 \quad (N)$$

This yields the ciphertext message $P(M)$=HSGAN. It can be checked by brute force that $P(x) = x \cdot_{26} 5$ is a one-to-one function (see handout).

To decrypt the message C=HSGAN, it appears that we should use the function $S(y) = x \cdot_{26} \frac{1}{5}$ (wrong); however, this function is NOT well defined since in the general the output yields a fraction. Thus, we need to reinterpret division by 5 as computing the *inverse* of 5 in $\mathbb{Z}_{26}$.

$P(x) = x \cdot_{26} 4$

(b) Then using encryption of multiplication by 4 mod 26 yields

$$P(17) = 17 \cdot_{26} 4 = 16 \quad (Q)$$
$$P(14) = 14 \cdot_{26} 4 = 4 \quad (D)$$
$$P(22) = 22 \cdot_{26} 4 = 10 \quad (K)$$
$$P(0) = 0 \cdot_{26} 4 = 0 \quad (A)$$
$$P(13) = 13 \cdot_{26} 4 = 0 \quad (A)$$

This yields the ciphertext message P(M)=QDKAA. Observe that $P(x) = x \cdot_{26} a$ is **NOT** a one-to-one function since $P(0) = P(13) = 0$ (see handout). there is repetition

PROBLEM: To have a valid decryption algorithm, it is therefore necessary to determine those values of a and n for which the cipher $P(x) = x \cdot_n a$ is a one-to-one function. This is the goal of the next section.

mod n

$P(x) = x \cdot_{26} a$ is one-to-one if a is relatively prime to 26

↳ shouldn't have a common factor w/ 26 EXCEPT 1

0 & 26 → NOT relatively prime

common factors: 1, 2

↑ greatest common divisor (GCD)

Ex. gcd(11, 26) = 1

$5^{-1} = 21 \pmod{26}$ →

$P(x) = x \cdot_{26} 5$ (one-to-one) → $P^{-1}(y) = y \cdot_{26} 21$

$P(x) = x \cdot_{26} 4$ (NOT one-to-one) → $P^{-1}(y) =$ DNE

① For what values of a & n does P(x) have an inverse?

② How to calculate x^{-1} if it exists?

2.2 Inverses and Greatest Common Divisors

Solutions to Equations and Inverses mod n

Definition: The *multiplicative inverse* of an integer a in $\mathbb{Z}_n$ is a number a' (also denoted by a^{-1}) that satisfies

$$a \cdot_n a' = 1$$

Example:

(a) The multiplicative inverse of 2 in $\mathbb{Z}_9$ equals 5 since $2 \cdot_9 5 = 1$. We also write $2^{-1} = 5$ (in $\mathbb{Z}_9$).

(b) The integer 3 does NOT have a multiplicative inverse in $\mathbb{Z}_9$ since the equation $3 \cdot_9 x = 1$ has no solutions (verify this by brute force).

Lemma: Suppose a has a multiplicative inverse a' in $\mathbb{Z}_n$. Then for any b in $\mathbb{Z}_n$, the equation

$$a \cdot_n x = b$$

has a unique solution in $\mathbb{Z}_n$ given by

$$x = a' \cdot_n b$$

Proof: We solve for x by multiplying both sides of the given equation by a':

$$a' \cdot_n (a \cdot_n x) = a' \cdot_n b$$
$$\Rightarrow (a' \cdot_n a) \cdot_n x = a' \cdot_n b$$
$$\Rightarrow 1 \cdot_n x = a' \cdot_n b$$
$$\therefore x = a' \cdot_n b$$

Example:

(a) The equation $2 \cdot_9 x = 7$ has solution

$$x = 2^{-1} \cdot_9 7 = 5 \cdot_9 7 = 5 \cdot 7 \bmod 9 = 8$$

Inverses mod n

Tables of Inverses:

$\mathbb{Z}_3$

a	1	2
a'	1	2

$\mathbb{Z}_4$

a	1	2	3
a'	1	-	3

$\mathbb{Z}_5$

a	1	2	3	4
a'	1	3	2	4

NATURAL QUESTIONS:

1. Which values of a have multiplicative inverses in $\mathbb{Z}_n$?
2. Which values of n have the property that every element in $\mathbb{Z}_n$ has a multiplicative inverse?

Corollary: Suppose there exists a value b in $\mathbb{Z}_n$ so that the equation

$$a \cdot_n x = b$$

has NO solution. Then a does NOT have a multiplicative inverse in $\mathbb{Z}_n$.

Proof: (by contradiction) Assume on the contrary that a has a multiplicative inverse a'. Then by the previous lemma the equation $a \cdot_n x = b$ has solution $x = a' \cdot_n b$, which contradicts the assumption that there are no solutions. Hence, a does not have a multiplicative inverse.

Principle of Proof by Contradiction: If by assuming a statement we want to prove is false leads us to a contradiction, then the statement we are trying to prove must be true.

Theorem: If an element in $\mathbb{Z}_n$ has a multiplicative inverse, then the inverse is unique, i.e. there is exactly one such inverse.

Proof: (by contradiction) Suppose on the contrary that a has two distinct inverses a' and a^*. Then

$$\begin{aligned} & a \cdot_n a' = 1 = a \cdot_n a^* \\ \Rightarrow\ & a' \cdot_n (a \cdot_n a') = a' \cdot_n (a \cdot_n a^*) \\ \Rightarrow\ & (a' \cdot_n a) \cdot_n a' = (a' \cdot_n a) \cdot_n a^* \\ \Rightarrow\ & 1 \cdot_n a' = 1 \cdot_n a^* \\ \therefore\ & a' = a^* \end{aligned}$$

But this contradicts the assumption that a' and a^* are distinct. Hence, there is only one such inverse.

Converting Modular Equations to Normal Equations

The modular equation $a \cdot_n x = 1$ can be rewritten in 'normal' form as follows:

$$a \cdot_n x = 1 \Rightarrow ax \bmod n = 1 \Rightarrow ax = nq + 1 \Rightarrow ax - nq = 1$$

Lemma: The equation $a \cdot_n x = 1$ has solution in $\mathbb{Z}_n$ if and only if there exists integers x and y satisfying the equation

$$ax + ny = 1$$

Proof: Set $y = -q$ in the previous derivation.

Example:
(a) The equation $2 \cdot_9 x = 1$ has solution in $\mathbb{Z}_9$ since there exists integers x and y satisfying the equation

$$2x + 9y = 1$$

In particular, $x = 5$ and $y = -1$.

(b) Does the equation $5 \cdot_{11} x = 1$ have a solution in $\mathbb{Z}_{11}$?

NOTE: Since solving the modular equation $a \cdot_n x = 1$ is equivalent to finding the inverse of a, we have the following theorem.

Theorem: A number a has a multiplicative inverse in $\mathbb{Z}_n$ if and only if there exists integers x and y satisfying the equation

$$ax + ny = 1$$

or equivalently,

$$a \cdot_n x = 1$$

Thus, $a^{-1} = x \bmod n$.

Example: The equation $2x + 9y = 1$ has infinitely many solutions, namely

$$(x, y) = \{(5,-1),(14,-3),(23,-5),\ldots,(-4,1),(-13,3),(-22,5),\ldots\}$$

However, the solution is unique if we restrict x to $\mathbb{Z}_9$:

$$2^{-1} = 5 = 14 \bmod 9 = 23 \bmod 9 = \ldots = -4 \bmod 9 = -13 \bmod 9 = -22 \bmod 9 = \ldots$$

Greatest Common Divisors

Consider the table of inverses for $\mathbb{Z}_{12}$:

a	1	2	3	4	5	6	7	8	9	10	11
a'	1	-	-	-	7	-	5	-	-	-	11

QUESTION: Which values of a have multiplicative inverses and why?

Definition: The *greatest common divisor d* (GCD) of two integers j and k is the largest positive integer d that divides into both j and k. We also write $\gcd(j,k)$ to denote the GCD d. If $\gcd(j,k) = 1$, then j and k are said to be *relatively prime*.

Theorem: Two integers a and n are relatively prime, i.e. $\gcd(a,n) = 1$, if and only if a has a multiplicative inverse in $\mathbb{Z}_n$.

We devote the rest of this section to proving this theorem. The following lemma establishes the reverse direction, which is easy to prove.

Lemma: If there exists integers x and y satisfying the equation

$$ax + ny = 1$$

then a and n are relatively prime, i.e. $\gcd(a,n) = 1$.

Proof: (by contradiction) Suppose on the contrary that $\gcd(a,n) = d > 1$. Then $a = dp$ and $n = dq$ for some integers p and q. It follows that

$$\begin{aligned} & ax + ny = 1 \\ \Rightarrow\ & (dp)x + (dq)y = 1 \\ \Rightarrow\ & d(px + qy) = 1 \end{aligned}$$

This shows that d is a divisor of 1, which is a contradiction since 1 cannot have divisors larger than 1.

As for proving the forward direction in the previous theorem, we shall require an algorithm to compute the GCD of two integers.

Euclid's Division Theorem (Restricted Version): Let n be a positive integer. Then for every *non-negative* integer m, there exist unique integers q and r such that $m = nq + r$ with $0 \le r < n$.

Proof: Refer to the textbook.

Example: Let $n = 24$ and $m = 90$. Then $90 = 24 \cdot 3 + 18$. Thus, $q = 3$ and $r = 18$.

NOTE: Observe that $\gcd(n,m) = \gcd(24,90) = \gcd(18,24) = \gcd(r,n)$ in the example above since the common factors of n and m are exactly the same as those for r and n. This result is true in general and the basis for Euclid's GCD algorithm.

Lemma: If j, k, q, and r are positive integers such that $k = jq + r$, then

$$\gcd(j,k) = \gcd(r,j)$$

Proof: We show that j and k have exactly the same common factors as r and j:

1. Let d be any factor of j and k. Then

$$\begin{aligned} & k = jq + r \\ \Rightarrow\ & r = k - jq \\ \Rightarrow\ & r = dt - (ds)q \\ \Rightarrow\ & r = d(t - sq) \end{aligned}$$

It follows that d is a factor of r (and also of j).

2. On the other hand, let d be any factor of r and j. Then

$$\begin{aligned} & k = jq + r \\ \Rightarrow\ & k = (du)q + dv \\ \Rightarrow\ & k = d(uq + v) \end{aligned}$$

It follows that d is a factor of k (and also of j). Thus, $\gcd(j,k) = \gcd(r,j)$.

NOTE: If $r = 0$, then $\gcd(k,j) = \gcd(r,j) = j$, e.g. $\gcd(6,12) = \gcd(0,6) = 6$.

Euclid's GCD Algorithm

The following algorithm computes $d = \gcd(j,k)$ with $j < k$:

1. Compute q and r from Euclid's Division Algorithm: $k = jq + r$
2. If $r > 0$, then replace (j,k) with (r,j) and repeat step 1.
3. Else $d = j$.

QUESTION: Why does this algorithm terminate?

Example: Let $j = 14$ and $k = 62$. Use Euclid's GCD algorithm to compute gcd(14,62).

(i) Step 1 yields

$$(j = 14, k = 62) \qquad 62 = 14 \cdot 4 + 6 \qquad (q = 4, r = 6)$$

(ii) Since $r > 0$ we replace (j,k) with (r,j) and repeat step 1:

$$(j = 6, k = 14) \qquad 14 = 6 \cdot 2 + 2 \qquad (q = 2, r = 2)$$

(iii) Since $r > 0$ we replace (j,k) with (r,j) and repeat step 1 again:

$$(j = 2, k = 6) \qquad 6 = 2 \cdot 3 + 0 \qquad (q = 3, r = 0)$$

(iv) Since $r = 0$ we stop. Thus, $d = j = \gcd(14,62) = \gcd(6,14) = \gcd(2,6) = 2$.

NOTE: We can summarize our results in table form below where the index i denotes values at the i-th step of the GCD algorithm:

i	$j[i]$	$k[i]$	$q[i]$	$r[i]$
0	14	62	4	6
1	6	14	2	2
2	**2**	6	3	0

Lemma: If j, k, q, r are positive integers such that $k = jq + r$ and x, y, x', y' are integers satisfying

$$jx + ky = \gcd(j,k) = \gcd(r,j) = rx' + jy'$$

then

$$x = y' - qx', \quad y = x'$$

Proof: We have

$$\gcd(r,j) = rx' + jy' = (k - jq)x' + jy' = kx' + j(y' - qx'), \quad \gcd(j,k) = jx + ky$$

Equating coefficients of j and k in both equations yields our desired formulas for x and y.

Extended GCD Algorithm

If $\gcd(j,k) = d$, then the following algorithm computes integers x and y that satisfy $jx + ky = d$:

1. Apply GCD algorithm to obtain table of values for $j[i]$, $k[i]$, $q[i]$, and $r[i]$ for $i = 0,1,\ldots,N$ where for the last step $j[N] = d$ and $r[N] = 0$.

2. Set $x[N]=1$ and $y[N]=0$.
3. Compute $x[i]$ and $y[i]$ for $i=N-1,N-2,...,0$ using the recursive formulas

$$\begin{cases} x[i]=y[i+1]-q[i]\cdot x[i+1] \\ y[i]=x[i+1] \end{cases}$$

4. Solution for x and y are given by $x[0]$ and $y[0]$, respectively.

Example: Find integers x and y that satisfy $14x+62y=\gcd(14,62)$:

Solution: From the previous example we found $d=\gcd(14,62)=2$. We now work backwards starting at the last step with $j[2]=2$, $k[2]=6$, $q[2]=3$, and $r[2]=0$ (here $N=2$):
(i) Set $x[2]=1$ and $y[2]=0$ since the following holds:

$$2=\gcd(2,6)=2\cdot 1+6\cdot 0$$

(ii) Next use the fact that $14=6\cdot 2+2$ from step $i=1$ to rewrite

$$\gcd(2,6)=2\cdot 1+6\cdot 0=(14-6\cdot 2\cdot)1+6\cdot 0=6(0-2\cdot 1)+14\cdot 1=6\cdot(-2)+14\cdot 1=\gcd(6,14)$$

(iii) Thus $x[1]=-2=0-2\cdot 1=y[2]-q[1]\cdot x[2]$ and $y[1]=1=x[2]$. Again, use the fact that $62=14\cdot 4+6$ from step $i=0$ to rewrite

$$\gcd(6,14)=6\cdot(-2)+14\cdot 1=(62-14\cdot 4)(-2)+14\cdot 1=14(1-4\cdot(-2))+62\cdot(-2)$$

(iv) Thus $x[0]=9=1-4\cdot(-2)=y[1]-q[0]\cdot x[1]$ and $y[0]=-2=x[1]$.
(v) We conclude that $x=x[0]=9$ and $y=y[0]=-2$.

NOTE: We can again summarize our work in table form where we take the table from the previous example, add columns for $x[i]$ and $y[i]$, and work upwards starting from the last step with $x[2]=1$ and $y[2]=0$ to obtain $x[0]$ and $y[0]$:

i	$j[i]$	$k[i]$	$q[i]$	$r[i]$	$x[i]=y[i+1]-q[i]\cdot x[i+1]$	$y[i]=x[i+1]$
0	14	62	4	6	$1-4\cdot(-2)=9$	–2
1	6	14	2	2	$0-2\cdot 1=-2$	1
2	**2**	6	3	0	1	0

Computing Inverses

Corollary: Two positive integers j and k are relatively prime, i.e. $\gcd(j,k)=1$, if and only if there exists integers x and y that satisfy $jx+ky=1$.

Corollary: For any positive integer n, an element a in $\mathbb{Z}_n$ has a multiplicative inverse if and only if a and n are relatively prime, i.e. $\gcd(a,n)=1$.

Corollary: For any prime p, every non-zero element a in $\mathbb{Z}_p$ has a multiplicative inverse.

Inverse Algorithm: The following algorithm solves the modular equation $a \cdot_n x = 1$ for x, i.e. finds the inverse of a (mod n):

1. Apply extended GCD algorithm to compute integers x and y satisfying $ax + ny = 1$ by setting $j = a$ and $k = n$.
2. The inverse is given by x (mod n).

Example: Find the inverse of 7 in $\mathbb{Z}_{26}$ if it exists.

Solution:

1. We use Euclid's GCD algorithm to check that $\gcd(7,26) = 1$:

i	$j[i]$	$k[i]$	$q[i]$	$r[i]$
0	7	26	3	5
1	5	7	1	2
2	2	5	2	1
3	**1**	2	2	0

Thus, the inverse of 7 exists.

2. Next we use Euclid's Extended GCD algorithm to find integers x and y satisfying $7x + 26y = 1$.

i	$j[i]$	$k[i]$	$q[i]$	$r[i]$	$x[i] = y[i+1] - q[i] \cdot x[i+1]$	$y[i] = x[i+1]$
0	7	26	3	5	$-2 - 3 \cdot 3 = \mathbf{-11}$	3
1	5	7	1	2	$1 - 1 \cdot (-2) = 3$	-2
2	2	5	2	1	$0 - 2 \cdot 1 = -2$	1
3	**1**	2	2	0	1	0

3. This shows that $x = -11$ and $y = 3$ (check that $7 \cdot (-11) + 26 \cdot 3 = 1$). Thus, the inverse of 7 is given by

$$7^{-1} = x \bmod n = -11 \bmod 26 = \boxed{15}$$

NOTE: This also checks with the fact that $7 \cdot_{26} 15 = 1$.

Example: Solve the modular equation $7x = 5 \bmod 26$ for x.

Solution: From the previous example, we know that $7^{-1} \bmod 26 = 15$. Thus, we can solve for x by multiplying through by 7^{-1}:

$$7x = 5 \bmod 26$$
$$\Rightarrow 7^{-1} \cdot 7x = 7^{-1} \cdot 5 \bmod 26$$
$$\Rightarrow x = 15 \cdot 5 \bmod 26$$
$$\therefore x = 23$$

2.3 The RSA (Rivest–Shamir–Adleman) Cryptosystem

Exponentiation mod n

$$b = a^j \bmod n$$

Key Generation: Bob does the following:

(1) Choose 2 large prime numbers p and q
(2) Set $n = p \cdot q$
(3) Choose integer $e \neq 1$ so that e is relatively prime to $m = (p-1)(q-1)$
(4) Compute $d = e^{-1} \bmod m$
(5) Keep d secret

ENCRYPTION: Alice does the following to send message x to Bob:

(1) Read the public directory for Bob's public keys e and n
(2) Compute $y = x^e \bmod n$
(3) Send encrypted message y to Bob

DECRYPTION: Bob does the following to read Alice's message:

(1) Receive encrypted message y from Alice
(2) Compute $z = y^d \bmod n$ using secret key d
(3) Read message z (same as x)

Example: Set $p = 13, q = 29$. Then

$$n = pq = 377$$
$$m = (p-1)(q-1) = 336$$

Choose public key $e = 187$ so that $\gcd(e,m) = \gcd(187,336) = 1$. Then private key is

$$d = e^{-1} \bmod m = 187^{-1} \bmod 336 = 115$$

Example:
(a) Can you factor the integer below into a product of primes?

$n = 474086162732884441412427976102263467817252574539006581970886780201234 2\$
1922311

(b) Given n in part (a) and the public key $e = 179424673$, can you break the encryption by finding the private key d?