Introduction to Number Theory and its Applications

"Mathematics is the queen of sciences and the theory of numbers is the queen of mathematics." (Karl Friedrich Gauss)

Introduction

In the next sections we will review concepts from **Number Theory**, the branch of mathematics that deals with integer numbers and their properties.

We will be covering the following topics:

1. Divisibility and Modular Arithmetic (applications to hashing functions/tables and simple cryptographic cyphers). Section 3.4
2. Prime Numbers, Greatest Common Divisors (GCD) and Euclidean Algorithm. Section 3.5, part of 3.6
3. Applications to computer science: computer arithmetic with large integers and cryptography. Section 3.7

Divisibility

When dividing an integer by a second nonzero integer, the quotient may or may not be an integer.
For example, $12/3 = 4$ while $9/4 = 2.25$.

The issue of divisibility is addressed in the following definition.

Definition

If a and b are integers with $a \neq 0$, we say that a *divides* b if there exists an integer c such that $b = ac$. When a divides b we say that a is a *factor* of b and that b is a *multiple* of a.
The notation $a \mid b$ denotes a divides b and $a \not\mid b$ denotes a does not divide b.

Back to the above examples, we see that 3 divides 12, denoted as $3 \mid 12$, and 4 does not divide 9, denoted as $4 \not\mid 9$.

Divisibility Properties

Theorem (1)

Let a, b, and c be integers. Then,

1. *if $a \mid b$ and $a \mid c$ then $a \mid (b + c)$;*
2. *if $a \mid b$ then $a \mid bc$ for all integers c;*
3. *if $a \mid b$ and $b \mid c$ then $a \mid c$;*

Proof: Direct proof given in class.

Corollary (1)

If a, b, and c are integers such that $a \mid b$ and $a \mid c$, then $a \mid mb + nc$ whenever m and n are integers.

Proof: Direct proof given in class.

The division algorithm

Theorem (2, The division algorithm)

Let a be an integer and d a positive integer. Then, there are unique integers q and r, with $0 \leq r < d$, such that $a = dq + r$.

- d is called the *divisor*;
- a is called the *dividend*;
- q is called the *quotient*; this can be expressed $q = a \textbf{ div } d$;
- r is called the *remainder*; this cane be expressed $r = a \textbf{ mod } d$;

Example:

If $a = 7$ and $d = 3$, then $q = 2$ and $r = 1$, since $7 = (2)(3) + 1$.
If $a = -7$ and $d = 3$, then $q = -3$ and $r = 2$, since $-7 = (-3)(3) + 2$.

Using successive subtractions to find q and r:

$a = 101$ and $d = 11$

$$\begin{array}{r} 101 \\ -\ 11 \\ \hline 90 \\ -\ 11 \\ \hline 79 \\ -\ 11 \\ \hline 68 \\ -\ 11 \\ \hline 57 \\ -\ 11 \\ \hline 46 \end{array} \qquad \begin{array}{r} 46 \\ -\ 11 \\ \hline 35 \\ -\ 11 \\ \hline 24 \\ -\ 11 \\ \hline 13 \\ -\ 11 \\ \hline 2 \end{array}$$

$q = 9$ as we subtracted 11, 9 times

$r = 2$ since this was the last value before getting negative.

Proof of the previous theorem (the division Algorithm)

Existence:
Let S be the set of nonnegative integers of the form $a - dq$, where q is an integer. This set is nonempty because $-dq$ can be made as large as desired (taking q as a negative integer with large absolute value). By the well-ordering property, S has a least element $r = a - dq_0$ for some integer q_0.
The integer r is nonnegative. It is also the case that $r < d$; otherwise if $r \geq d$, then there would be a smaller nonnegative element in S, namely $a - d(q_0 + 1)$, contradicting the fact that $a - dq_0$ was the smallest element of S. So, we just proved the existence of r and q, with $0 \leq r < d$. $\square$

Uniqueness:
Suppose there exist q, Q, r, R with $0 \leq r, R < d$ such that $a = dq + r$ and $a = dQ + R$. Assume without loss of generality that $q \leq Q$. Subtracting both equations, we have $d(q - Q) = (R - r)$. Thus, d divides $(R - r)$, and so $|d| < |(R - r)|$ or $R - r = 0$. But we know that $0 \leq r, R < d$, so $|R - r| < d$, and we must have $R - r = 0$. This means $R = r$, which substituting into original equations gives $a - r = dq = dQ$. Since $d \neq 0$, dividing both sides of $dq = dQ$ by d we get that $q = Q$. Therefore we have showed that $r = R$ and $q = Q$, proving uniqueness. $\square$

Modular Arithmetic

Definition

If a and b are integers and m is a positive integer, then a is *congruent to* b *modulo* m if m divides $a - b$. We use the notation $a \equiv b \pmod{m}$ if this is the case, and $a \not\equiv b \pmod{m}$, otherwise.

The following theorem says that two numbers being congruent modulo m is equivalent to their having the same remainders when dividing by m.

Theorem (3)

Let a and b be integers and let m be a positive integer. Then, $a \equiv b \pmod{m}$ if and only if $a \mathbf{\ mod\ } m = b \mathbf{\ mod\ } m$.

Example: 10 and 26 are congruent modulo 8, since their difference is 16 or -16, which is divisible by 8. When dividing 10 and 26 by 8 we get $10 = 1 \cdot 8 + 2$ and $26 = 4 \cdot 8 + 2$. So $10 \mathbf{\ mod\ } 8 = 2 = 16 \mathbf{\ mod\ } 8$.

Proof of the theorem given in class.

(you may use this space to take notes)

Theorem (4)

Let m be a positive integer. The integers a and b are congruent modulo m if and only if there is an integer k such that $a = b + km$

(Proof given in class.)

Theorem (5)

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

(Proof given in class.)

Corollary (2)

Let m be a positive integer and let a and b be integers. Then,

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

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

Proof:
By the definition of $\textbf{mod } m$ and the definition of congruence modulo m, we know that $a \equiv (a \textbf{ mod } m) \pmod{m}$, and $b \equiv (b \textbf{ mod } m) \pmod{m}$. Applying Theorem 5, we get

$$a+b \equiv (a \textbf{ mod } m) + (b \textbf{ mod } m) \pmod{m}$$

$$ab \equiv (a \textbf{ mod } m)(b \textbf{ mod } m) \pmod{m}$$

Using Theorem 3, from the above congruences we get the equalities in the statement of the theorem.

Congruences and Hashing Functions

A **hashing table** is a data structure that allows for direct access to data. If done carefully, and under certain assumptions, we can search for a record with a set of n records in expected time $O(1)$.
Each record is uniquely identified by a key (e.g. of keys are student number for a student record, account number for bank account records, call number for book records in a library, etc).

One of the most common hash functions uses modular arithmetic: $h(k) = k \textbf{ mod } m$, where m is the number of memory addresses.
Advantages: easy to compute, function is onto (all memory address can be used).

Since two different integers k_1 and k_2 may be mapped to the same location if $k_1 \equiv k_2 \pmod{m}$, **collisions** may arises. Methods for finding an alternate location for a key are employed (collision resolution techniques).

Congruences and Pseudorandom Number Generators

We need random numbers in several types of algorithms, such as: **randomized algorithms**: algorithms that need to flip a coin to behave unbiasedly), **simulation algorithms**: where probability models are used to explain behaviour (example: arrival rate of subway passengers).

A systematic method of generating a number cannot be truly random, so we call them **pseudorandom number generators**. The most common method for such generators is the **linear congruential method**.

Pick integers a, c, m and seed x_0, with $2 \leq a < m$, $0 \leq c, x_0 < m$.

Generate a sequence of numbers $x_0, x_1, x_2, \ldots$ from the seed x_0, using the congruence:

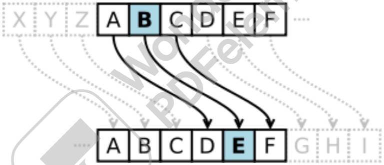
$$x_{n+1} = (ax_n + c) \textbf{ mod } m.$$

The length of the period before repeats is called the **period**. Of course the period is at most m, and sometimes is exactly m (see textbook example). For this reason m must be large.

If we need a number in $[0, 1]$ we simply provide x_n/m.

Congruences and Cryptography

Cryptology is the study of secret messages. One of its early uses was by Roman emperor Julius Caesar.
The Caesar cipher shifted each letter 3 letters forward in the alphabet (cyclically, sending xyz to abc respectively):



Decipher the message: JRRG OXFN LQ WKH PLGWHUP!
We can express the Caesar cipher mathematically using modular arithmetic (and generalizing the shift by 3 to a shift by k):

encryption function: $f(p) = (p + k) \textbf{ mod } 26.$
decryption function: $f^{-1}(p) = (p - k) \textbf{ mod } 26$

Primes

Definition

A positive integer $p > 1$ is called *prime* if the only positive factors of p are 1 and p. A positive integer that is greater than one and is not prime is called *composite*.

An integer n is composite if and only if there exists an integer a such that $a|n$ and $1 < a < n$.

Prime numbers: 2, 3, 5, 7, 11, 13, 17, etc.

For the following composite numbers n provide a proof it is composite, that is, give a divisor a, with $1 < a < n$:
Composite Numbers: 4, 6, 8, 9, 10, 12, 14, 15, etc.

Theorem (The Fundamental Theorem of Arithmetic)

Every positive 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 order of nondecreasing size.*

The proof uses strong induction, so we will delay it until the next topic.

Examples:

$$\begin{aligned} 100 &= 2 \cdot 2 \cdot 5 \cdot 5 = 2^2 \cdot 5^2 \\ 641 &= 641 \\ 333 &= 3 \cdot 3 \cdot 37 = 3^2 \cdot 37 \\ 64 &= 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2^6 \end{aligned}$$

Theorem

If n is a composite integer, then n has a prime divisor less than or equal to $\sqrt{n}$.

Proof: If n is composite then n has a factor a with $1 < a < n$. So, there exists an integer $b > 1$ such that $n = ab$. We claim that $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$. Indeed, assuming by contradiction that $a > \sqrt{n}$ and $b > \sqrt{n}$, we would get $n = ab > \sqrt{n} \cdot \sqrt{n} = n$, a contradiction. So, $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$. Thus, n has a positive divisor $\leq \sqrt{n}$. If the divisor d is prime, then the theorem follows. If the divisor d is composite, then by the Fundamental Theorem of Arithmetic, it has a prime divisor $p < d \leq \sqrt{n}$, and since $p|d$ and $d|n$, we have that p divides n, and the theorem follows in this case as well. $\square$

Exercise: Use this Theorem to show 101 is prime.

Theorem

There are infinitely many primes.

Proof: We will use a proof by contradiction. Assume there are finitely many primes: $p_1, p_2, \ldots, p_n$. Let $Q = p_1 p_2 \cdots p_n + 1$.
By the Fundamental Theorem of Arithmetic, Q is prime or it can be written as the product of two or more primes. In either case, there exists a prime p such that $p|Q$.
We claim this prime p cannot be any of the p_i with $1 \leq i \leq n$. Indeed, if $p_i|Q$, we would conclude that $p_i|(Q - p_1 p_2 \cdots p_n) = 1$, which is a contradiction. Therefore, we conclude that p is a prime, and is not any of the primes listed $p_1, p_2, \ldots, p_n$. But we have assumed that this was a complete list of all existing primes, and we reached a contradiction.
$\square$

Greatest Common Divisors

Definition

Let a and b be integers, not both zero. The largest integer d such that $d|a$ and $d|b$ is called the *greatest common divisor* of a and b, and is denoted by gcd(a, b).

Example: The positive common divisors of 24 and 36 are $1, 2, 3, 4, 6, 12$.
So, gcd$(24, 36) = 12$.

Find the following greatest common divisors:
gcd$(17, 100) =$
gcd$(1000, 625) =$

Definition

The integers a and b are *relatively prime* if $\gcd(a, b) = 1$.

8 and 9 are relatively prime since $8 = 2^3$ and $9 = 3^2$, their only common divisor is 1, giving $\gcd(8, 9) = 1$.

Are the following numbers relatively prime?

- 3 and 12
- 1024 and 625
- 7 and 15

Proposition

Let a and b be positive integers and let $p_1, p_2, \ldots, p_n$ be all the primes that appear in the prime factorization of a or b, so that

$$a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}, \qquad b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n},$$

where each $a_i, b_i \geq 0$ for $1 \leq i \leq n$. Then,

$$\gcd(a,b) = p_1^{\min(a_1,b_1)} p_2^{\min(a_2,b_2)} \cdots p_n^{\min(a_n,b_n)}$$

Proof: First note that the integer $d = p_1^{\min(a_1,b_1)} p_2^{\min(a_2,b_2)} \cdots p_n^{\min(a_n,b_n)}$ divides a and b, since the power of each prime p_i does not exceed the power of p_i appearing in the factorization of each of these numbers. Second, the exponents of p_i in d cannot be increased, otherwise it would not divide one of a or b, and no other prime can be included. $\square$

Example: $120 = 2^3 \cdot 3 \cdot 5$ and $500 = 2^2 \cdot 5^3$,
so $\gcd(120, 500) = 2^{\min(3,2)} 3^{\min(1,0)} 5^{\min(1,3)} = 2^2 3^0 5^1 = 20$.

Definition

The *least common multiple* of the positive integers a and b is the smallest positive integer that is divisible by both a and b, denoted by $\text{lcm}(a, b)$.

Examples: $\text{lcm}(2, 10) = 10$, $\text{lcm}(5, 7) = 35$, $\text{lcm}(4, 6) = 12$.

Proposition

Let a and b be positive integers and let $p_1, p_2, \ldots, p_n$ be all the primes that appear in the prime factorization of a or b, so that

$$a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}, \qquad b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n},$$

where each $a_i, b_i \geq 0$ for $1 \leq i \leq n$. Then,

$$\text{lcm}(a, b) = p_1^{\max(a_1,b_1)} p_2^{\max(a_2,b_2)} \cdots p_n^{\max(a_n,b_n)}$$

Proof: left as exercise (similar to the previous proposition)

Theorem

Let a and b be positive integers. Then,

$$ab = \gcd(a,b) \cdot \operatorname{lcm}(a,b).$$

Proof: Write a and b as in the previous propositions

$$a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}, \qquad b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n},$$

By these propositions, we have
$\gcd(a,b) \cdot \operatorname{lcm}(a,b) =$
$(p_1^{\min(a_1,b_1)} p_2^{\min(a_2,b_2)} \cdots p_n^{\min(a_n,b_n)})(p_1^{\max(a_1,b_1)} p_2^{\max(a_2,b_2)} \cdots p_n^{\max(a_n,b_n)})$
$= p_1^{\max(a_1,b_1)+\min(a_1,b_1)} p_2^{\max(a_2,b_2)+\min(a_2,b_2)} \cdots p_n^{\max(a_n,b_n)+\min(a_n,b_n)}.$
Now note that $\max(a_i,b_i) + \min(a_i,b_i) = a_i + b_i$. Thus,

$$\begin{aligned} \gcd(a,b) \cdot \operatorname{lcm}(a,b) &= p_1^{a_1+b_1} p_2^{a_2+b_2} \cdots p_n^{a_n+b_n} \\ &= p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n} p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n} = ab. \end{aligned}$$

Towards an efficient GCD Algorithm

The methods described in Proposition 1 to calculate gcd(a, b) via the prime factorization of a and b is not efficient.
For instance, we do not know how to efficiently factor a number; that is, there are no polynomial time algorithm known that does this job. Since that method requires factoring a and b, we would need to use algorithms that do not run in polynomial time (exponential or sub-exponential time).

Note that here the input size is $\lfloor \log_2 a \rfloor + \lfloor \log_2 b \rfloor$ (number of bits needed to represent a and b). An algorithm running in linear time with a and b would not be a polynomial time algorithm.
However, there is an efficient algorithm which uses only $O(\log(\min(a, b)))$ integer divisions.
This algorithm was invented by Euclid, a famous mathematician living during 325-265 B.C.

The Euclidean Algorithm

We want to calculate the gcd$(91, 287)$.
Applying the division algorithm to 287 and 91, we get

$$287 = 91 \cdot 3 + 14.$$

Any common divisor d of 287 and 91 must also be a divisor of 14, because $d|287$ and $d|91$ implies $d|(287 - 91 \cdot 3) = 14$.
Also, any common divisor of 91 and 14 must also be a divisor of 287.
So, gcd$(287, 91)$=gcd$(91, 14)$. Great! We've just decreased one of the numbers. Continue the process by dividing 91 by 14:

$$91 = 14 \cdot 6 + 7.$$

Again, we conclude gcd$(91, 14)$=gcd$(14, 7)$, and divide 14 by 7:

$$14 = 7 \cdot 2 + 0$$

Because 7 divides 14 we know gcd$(14, 7) = 7$. Therefore, gcd$(287, 91)$ =gcd$(91, 14)$ =gcd$(14, 7) = 7$.

The Euclidean algorithm is based on the following Lemma:

Lemma

Let $a = bq + r$ where a, b, q and r are integers. Then gcd(a, b) =gcd(b, r).

Proof: It is enough to show that the common divisors of a and b are the same as the common divisors of b and r, for then they will also share the *greatest* common divisor.
Suppose $d|a$ and $d|b$. Then $d|a - bq = r$. So any common divisor of a and b is also a common divisor of b and r.
Suppose $d|b$ and $d|r$. Then $d|bq + r = a$ So, any common divisor of b and r is a common divisor of a and b.
Therefore, gcd(a, b) =gcd(b, r). □

The Euclidean Algorithm

Correctness of the Algorithm: partial correctness +termination

```
Input:  a and b positive integers
Output:  gcd(a,b)
   x := max(a,b)
   y := min(a,b)
   gcd(x,y)=gcd(a,b)
   while ($y \neq 0$) do   Loop invariant:  gcd(x,y)=gcd(a,b)
     r := x mod y     by the previous THM: gcd(x,y)=gcd(y,r)
     x:=y
     y:=r
   endwhile (loop terminates since $y \geq 0$ and decreases at each iteration)
   postcondition gcd(x,y)=gcd(a,b) and y=0
   postcondition x=gcd(x,0)=gcd(a,b)
   return x
```

Applying Euclidean Algorithm to find $\gcd(123, 277)$:

$$\begin{aligned} 277 &= 123 \cdot 2 + 31 \\ 123 &= 31 \cdot 3 + 30 \\ 31 &= 30 \cdot 1 + 1 \\ 30 &= \underline{1} \cdot 30 + 0 \\ \gcd(123, 277) &= 1 \end{aligned}$$

x	277	123	31	30	1 $\leftarrow$ gcd
y	123	$31_{=277 \bmod 123}$	$30_{=123 \bmod 31}$	$1_{=31 \bmod 30}$	$0_{=30 \bmod 1}$

Useful Results

Theorem (A)

If a and b are positive integers, then there exist integers s and t such that gcd$(a, b) = sa + tb$.

Example:
gcd$(252, 198) = 18 = 4 \cdot 252 - 5 \cdot 198$

We won't prove this now, but will show a method for computing s and t called the extended Euclidean Algorithm.

Extended Euclidean Algorithm

Consider the steps of the Euclidean algorithm for $\gcd(252, 198)$:

$$\begin{aligned} 252 &= 1 \cdot 198 + 54 \\ 198 &= 3 \cdot 54 + 36 \\ 54 &= 1 \cdot 36 + 18 \\ 36 &= 2 \cdot 18 \end{aligned}$$

Isolate the nonzero remainders in the above equations, substituting backwards:

$$\begin{aligned} \gcd(252, 198) = 18 &= 54 - 1 \cdot 36 \\ &= 54 - 1(198 - 3 \cdot 54) = 4 \cdot 54 - 1 \cdot 198 \\ &= 4 \cdot (252 - 1 \cdot 198) - 1 \cdot 198 = 4 \cdot 252 - 5 \cdot 198 \end{aligned}$$

Therefore, $\gcd(252, 198) = 4 \cdot 252 - 5 \cdot 198$.

Lemma (A)

If a, b, and c are positive integers such that gcd$(a, b) = 1$ and $a|bc$, then $a|c$.

Proof: Using Extended Euclidean Algorithm, there exists s and t such that $sa + tb = 1 =$gcd(a, b). Multiplying by c, we get $sac + tbc = c$. Since $a|bc$ then $a|tbc$. But then by the above equation since $a|sac$ and $a|tbc$, we get that $a|c$. $\square$

The above Lemma generalizes to the following Lemma:

Lemma (B)

If p is a prime and $p|a_1 a_2 \cdots a_n$, where each a_i is an integer, then $p|a_i$ for some i.

Proof: Do as an exercise.

Dividing both sides of a congruence

As we have seen, we can't always divide both sides of a congruence by the same integer, even if it is non-zero.

For example:
$6 \equiv 12 \pmod{6}$, but $3 \not\equiv 6 \pmod{6}$.
$14 \equiv 8 \pmod{6}$, but $7 \not\equiv 4 \pmod{6}$.

However, we can divide by appropriate integers c, as long as $\gcd(c, m) = 1$:

Theorem (B)

Let m be a positive integer and let a, b, and c be integers. If $ac \equiv bc \pmod{m}$ and $\gcd(c, m) = 1$, then $a \equiv b \pmod{m}$.

Proof: Since $ac \equiv bc \pmod{m}$ we have that $m | ac - bc = c(a - b)$. By Lemma A, since $\gcd(c, m) = 1$, we have that $c | (a - b)$. This gives $a \equiv b \pmod{m}$. $\square$

Solving Linear Congruences

Let m be a positive integer, a and b be integers and x be a variable. The following congruence is called a **linear congruence**:

$$ax \equiv b \pmod{m}.$$

How can we solve it, i.e. find all integers x that satisfy it?

One possible method is to multiply both sides of the congruence by an inverse $\overline{a}$ of $a \pmod{m}$ if one such inverse exists:
$\overline{a}$ is an **inverse** of $a \pmod{m}$ if $\overline{a}a \equiv 1 \pmod{m}$.

Example:
5 is an inverse of $3 \pmod 7$, since $5 \cdot 3 \equiv 15 \equiv 1 \pmod 7$.
Using this we can solve:

$$\begin{aligned} 3x &\equiv 4 \pmod 7 \\ 5 \cdot 3x &\equiv 5 \cdot 4 \pmod 7 \\ 1 \cdot x &\equiv 20 \pmod 7 \\ x &\equiv 6 \pmod 7 \end{aligned}$$

Substitute back into the original linear congruence to check that 6 is a solution:

$$3 \cdot 6 \equiv 18 \equiv 4 \pmod 7.$$

But how can we compute inverses $\pmod m$?

Computing inverses modulo m

Theorem

If a and m are relatively prime integers with $m > 1$, then an inverse of a modulo m exists. Furthermore, this inverse is unique modulo m.

Proof: By Theorem A, since $\gcd(a, m) = 1$, there exists s and t such that

$$sa + tm = 1.$$

This implies $sa + tm \equiv 1 \pmod{m}$. Since $tm \equiv 0 \pmod{m}$, so $sa \equiv 1 \pmod{m}$, which implies s is an inverse of a modulo m.
It remains to show that this inverse is unique modulo m. Suppose s and s' are inverses of a modulo m. Then,

$$sa \equiv 1 \equiv s'a \pmod{m}.$$

Since $\gcd(a, m) = 1$, by Theorem B, we can divide both sides of the congruence by a, obtaining $s \equiv s' \pmod{m}$. $\square$

Computing the inverse of 24 modulo 7

Applying the extended Euclidean Algorithm:

$$\begin{aligned} 24 &= 3 \cdot 7 + 3 \\ 7 &= 2 \cdot 3 + 1 \\ 3 &= 3 \cdot 1 + 0 \end{aligned}$$

Using backward substitution:

$$1 = 7 - 2 \cdot 3 = 7 - 2 \cdot (24 - 3 \cdot 7) = -2 \cdot 24 + 7 \cdot 7.$$

So $s = -2$ and $t = 7$.

$$-2 \cdot 24 \equiv 1 \pmod{7}$$

You can use as an inverse of 24 modulo 7, any integer equivalent to -2 modulo 7, such as: $\ldots, -9, -2, 5, 12, 19, \ldots$

Chinese Remainder Thm: solving systems of congruences

A Chinese Mathematician asked in the first century:

> *There are certain things whose number is unknown. When divided by* 3*, the remainder is* 2*; when divided by* 5 *the remainder is* 3*; and when divided by* 7*, the remainder is* 2*. What will be the number of things?*

This puzzle is asking for the solution of the following system of congruences:

$$\begin{aligned} x &\equiv 2 \pmod 3, \\ x &\equiv 3 \pmod 5, \\ x &\equiv 2 \pmod 7. \end{aligned}$$

The Chinese Remainder Theorem establishes that when the moduli are pairwise relatively prime, we can solve such as system of linear congruences uniquely module the product of the moduli.

Theorem (Chinese Reminder Theorem)

Let $m_1, m_2, \ldots, m_n$ be pairwise relatively prime positive integers and $a_1, a_2, \ldots, a_n$ be arbitrary integers. Then, the system:

$$\begin{aligned} x &\equiv a_1 \pmod{m_1}, \\ x &\equiv a_2 \pmod{m_2}, \\ \ldots & \quad \ldots \\ x &\equiv a_n \pmod{m_n}, \end{aligned}$$

has a unique solution modulo $m = m_1 m_2 \ldots m_n$. (That is, there is a solution x with $0 \le x < m$, and all other solutions are congruent modulo m to this solution).

Proof of the Chinese Reminder Theorem (existence part)

In order to construct a simultaneous solution, let $M_k = m/m_k$. Note that $gcd(m_k, M_k) = 1$. So there exists y_k inverse of M_k modulo m_k.
Then $x = a_1M_1y_1 + a_2M_2y_2 + \cdots + a_nM_ny_n$ is a simulatneous solution.
Indeed, for any $1 \leq k \leq n$, since for $j \neq k$, all terms except kth term are 0 modulo m_k, which gives $x \equiv a_2M_ky_k \equiv a_k \pmod{m_k}$. $\square$
Showing that this is a unique solution is exercise 3.7-24, which is recommended.
Solving the original old question, that asks for a simultaneous solution to
$x \equiv 2 \pmod 3$, $x \equiv 3 \pmod 5$, $x \equiv 2 \pmod 7$.
$m_1 = 3$, $m_2 = 5$, $m_3 = 7$, so $m = m_1m_2m_3 = 105$.
$a_1 = 2$, $a_2 = 3$, $a_3 = 2$;
$M_1 = 35$, an inverse of 35 modulo 3: 2 $M_2 = 21$, an inverse of 21 modulo 5: 1 $M_3 = 15$. an inverse of 35 modulo 3: 1
So the solution $x \equiv a_1M_1y_1 + a_2M_2y_2 + a_3M_3y_3 \equiv$
$2 \cdot 25 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 \equiv 233 \equiv 23 \pmod{105}$.

Fermat's Little Theorem

Theorem (Fermat's Little Theorem)

If p is a prime and a is an integer not divisible by p, then

$$a^{p-1} \equiv 1 \pmod{p}.$$

Furthermore, for every integer a we have

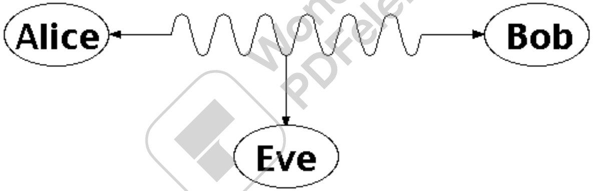
$$a^p \equiv a \pmod{p}.$$

The proof is left as an exercise, whose steps are outlined in Exercise 17 (page 244-245).

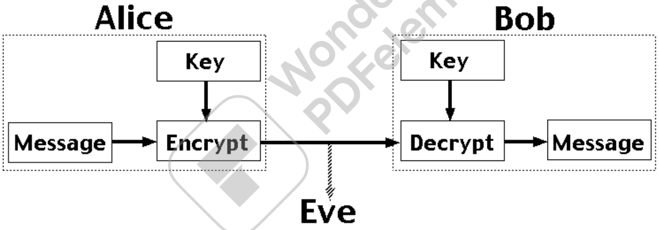
Example: $p = 5$
Verify that the theorem works for $a = 1, 2, 3, 4$: For 1 it is trivial,
$2^4 = 16 \equiv 1 \pmod 5$, $3^4 = 81 \equiv 1 \pmod 5$, $4^4 = 256 \equiv 1 \pmod 5$.

Public Key Cryptography and the RSA Cryptosystem

Two people, say Alice and Bob, would like to exchange secret messages; however, Eve is eavesdropping:



One technique would be to use an encryption technique based on an **encryption key**, but this poses a challenge: how do they exchange the encryption key without Eve receiving it?



Traditional Cryptography

In normal cryptography, both parties need to know a secret key k. The sender then encodes message m using key k via some method f to get the ciphertext c:

$$c = f(m, k).$$

Then, the receiver decodes the ciphertext c using key k via some method g to get back the original message m:

$$m = g(c, k).$$

The issue here is how to securely exchange the secret key k.

If we could find a method of encryption / decryption such that exchanging the necessary keys does not reveal to Eve how to decrypt intercepted messages, then we would avoid this problem altogether.

Public Key Cryptosystem

The idea is that the receiver publically publishes a **public key** k. Then anyone who wishes to encode a message m can do so:

$$c = f(m, k).$$

The receiver has a **private key** k' that is needed to decode the ciphertext c to receive the original message m:

$$m = g(c, k).$$

Both the encoding technique f and the decoding technique g are also publically known; the only secret information is k'.

While it is possible, it is computationally difficult to compute k' from k: the **key pair** can be chosen so that in the amount of time it takes to derive k' from k, the information m no longer has significant value.

RSA Cryptosystem

The most common form of public key cryptosystem is RSA, which stands for Rivest, Shamir, and Adleman, who invented it. It is based on modular arithmetic and large primes, and its security comes from the computational difficulty of factoring large numbers.

The idea is as follows: select p and q to be large primes (at least several hundred digits); the degree of security is dependent on the size of p and q. Take $n = pq$. Then the **public key** is a pair $k = (n, e)$ such that:

$$\gcd(e, (p-1)(q-1)) = 1.$$

The **encoding function** is:

$$f(m, k) \equiv m^e \pmod{n}.$$

This assumes that the message can be represented by an integer $m < n$ with $\gcd(m, p) = \gcd(m, q) = 1$; if not, we can break m down into smaller pieces and encode each individually.

The **private key** is a pair $k' = (n, d)$ such that:

$$de \equiv 1 \pmod{(p-1)(q-1)}.$$

The **decoding function** is:

$$g(c, k') = c^d \pmod{n}.$$

The security of the algorithm lies in the challenge of **prime factorization**: in order to calculate d, it is necessary to factor n to get p and q, which is very difficult (exponential in the number of digits in p and q).

We now proceed to show that RSA actually works.

Proof of the RSA Cryptosystem

Theorem (RSA Cryptosystem)

Let p, q *be primes with* $n = pq$ *and let* e *be an integer such that* $\gcd(e, (p-1)(q-1)) = 1$, *with* $ed \equiv 1 \pmod{(p-1)(q-1)}$. *Let* m *be an integer with* $m < n$ *and* $\gcd(m, p) = \gcd(m, q) = 1$. *Define* $k = (n, e)$ *and* $k' = (n, d)$, *and the functions:*

$$f(m, k) = m^d \pmod{n}$$

$$g(c, k) = c^e \pmod{n}.$$

Then we claim that:

$$g(f(m, k), k') = m.$$

Proof.

We have that:

$$g(f(m,k),k') = (m^e \bmod n)^d \bmod n = m^{ed} \bmod n.$$

By the choice of e and d, we have that: $ed \equiv 1 \pmod{(p-1)(q-1)}$, or, equivalently, for some integer s, $ed = 1 + s(p-1)(q-1)$. By Fermat's Little Theorem, $m^{p-1} \equiv 1 \pmod{p}$ and $m^{q-1} \equiv 1 \pmod{q}$, giving:

$$m^{ed} \equiv m^{1+s(p-1)(q-1)} \equiv m \cdot (m^{p-1})^{s(q-1)} \equiv m \cdot 1^{s(q-1)} \equiv m \pmod{p}.$$

Similarly, $m^{ed} \equiv m \pmod{q}$. Since $\gcd(p,q) = 1$, by the Chinese Remainder Theorem, $m^{ed} = m \pmod{pq}$ as required. □

Note that we can apply the same argument to show that:

$$f(g(m, k'), k) = m.$$

Thus, the owner of the private key can encrypt a message m using the private key, which can then be decrypted by anyone using the public key, and prove that only the private key owner could have encrypted it. This is the basis of **digital signature systems**.

Example: Bob wants to receive messages from Alice, so he selects two primes, say $p = 43$ and $q = 59$. (We choose small primes for feasibility of the example; in reality, they would be vastly larger.) Then $n = pq = 2537$ and $(p-1)(q-1) = 2436$. He then picks $e = 13$, which has the property that:

$$\gcd(e, (p-1)(q-1)) = \gcd(13, 2436) = 1.$$

Bob then calculates $d = 937$, the inverse of e mod 2436:

$$de \equiv 937 \times 13 \equiv 12181 \equiv 5 \times 2436 + 1 \equiv 1 \pmod{2436}.$$

Bob publishes the **public key** $k = (2537, 13)$.

Alice wants to send message “STOP” to Bob using RSA. She encodes this: S $\rightarrow 18$, T $\rightarrow 19$, O $\rightarrow 14$, P $\rightarrow 15$, i.e. 1819 1415 grouped into blocks of 4. Thus, $m = m_1 m_2 = 18191415$. Each block is encrypted:

$$1819^{13} \text{ mod } 2537 = 2081$$

$$1451^{13} \text{ mod } 2537 = 2182$$

Then the encrypted message is 20812182. Bob has **private key** $k' = (2537, 937)$, and computes:

$$2081^{937} \text{ mod } 2537 = 1819 \rightarrow \text{ST}$$

$$2812^{937} \text{ mod } 2537 = 1415 \rightarrow \text{OP}$$

Thus, the original message was STOP.