Number Theory

Theoretical Underpinnings of Modern Cryptography

Number Theory

- Theorem 1. Let a, b, c be integers. Then
  - if $a \mid b$ and $a \mid c$, then $a \mid (b+c)$ and $a \mid (b - c)$
  - if $a \mid b$ then $a \mid bc$, for all integers c
  - If $a \mid b$ and $b \mid c$ then $a \mid c$.
- Corollary 1. If $a \mid b$ and $a \mid c$, for integers a, b, c then for any integers x and y, $a \mid (bx + cy)$. The expression $bx + cy$ will be called a linear combination of b and c.
- We will use this later with gcd.

Number Theory

- Theorem 2. The division Algorithm. Let a and d be integers with $d > 0$. Then there are unique integers q and r, with $0 <= r < d$, such that $a = dq + r$.
  - d is the divisor
  - q is the quotient
  - r is the remainder.
- Definition 2. The notation used to find q and r is:
  - q = a div d, r = a mod d, where div is integer division (a / d in C , for int a, d)

Number Theory

- Example. What are q and r when 101 is divided by 11.
- Solution. We have 101 = 11*9 + 2. So q = 101 div 11 = 9, and r = 101 mod 11 = 2.
- Example. What are q and r when -11 is divided by 3.
- Solution. We have -11 = 3(-4) + 1.Note that remainder cannot be negative, and so r is not -2, because r= -2does not satisfy0 <= r < 3.
- Note. That a is divisible by d, if and only if r = 0.
- Sometimes we are only interested in the remainder.

MODULAR ARITHMETIC NOTATION

Given **any** integer a and a **positive** integer n, and given a division of a by n that leaves the remainder between 0 and $n-1$, both inclusive, we define

$$a \; mod \; n$$

to be **the remainder**. Note that the remainder **must** be between 0 and $n-1$, both ends inclusive, even if that means that we must use a negative quotient when dividing a by n.

We will call two integers a and b to be **congruent modulo n** if

$$(a \ mod \ n) \quad = \quad (b \ mod \ n)$$

Symbolically, we will express such a **congruence** by

$$a \quad \equiv \quad b \ \ (mod \ n)$$

We say a non-zero integer a is a **divisor** of another integer b provided there is no remainder when we divide b by a. That is, when $b \ = \ ma$ for some integer m.

When a is a divisor of b, we express this fact by $a \mid b$.

Examples of Congruences

Here are some congruences modulo 3:

$$
\begin{aligned}
7 &\equiv 1 \ (mod 3) \\
-8 &\equiv 1 \ (mod 3) \\
-2 &\equiv 1 \ (mod 3) \\
7 &\equiv -8 \ (mod 3) \\
-2 &\equiv 7 \ (mod 3)
\end{aligned}
$$

One way of seeing the above congruences (for mod 3 arithmetic):

...	0	1	2	0	1	2	0	1	2	0	1	2	0	1	2	0	1	2	0	1	2	0	...
...	-9	-8	-7	-6	-5	-4	-3	-2	-1	0	1	2	3	4	5	6	7	8	9	10	11	12	...

where the top line is the output of **modulo 3** arithmetic and the bottom line the set of **all** integers. [The top entry in each column is the modulo 3 value of the bottom entry in the same column. Pause for a moment and think about the fact that whereas $(7 \ mod \ 3) = 1$ on the positive side of the integers, on the negative side we have $(-7 \ mod \ 3) = 2$.]

Obviously, then, **modulo n** arithmetic maps all integers into the set $\{0, 1, 2, 3, ..., n-1\}$.

MODULAR ARITHMETIC OPERATIONS

As mentioned on the previous page, **modulo n** arithmetic maps all integers into the set $\{0, 1, 2, 3, ..., n-1\}$.

With regard to the modulo n arithmetic operations, the following equalities are easily shown to be true:

$$
\begin{aligned}
[(a \ mod \ n) \ + \ (b \ mod \ n)] \ mod \ n &= (a \ + \ b) \ mod \ n \\
[(a \ mod \ n) \ - \ (b \ mod \ n)] \ mod \ n &= (a \ - \ b) \ mod \ n \\
[(a \ mod \ n) \ \times \ (b \ mod \ n)] \ mod \ n &= (a \ \times \ b) \ mod \ n
\end{aligned}
$$

with ordinary meanings ascribed to the arithmetic operators.

To prove any of the above equalities, you write a as $mn + r_a$ and b as $pn + r_b$, where r_a and r_b are the **residues** (the same thing as **remainders**) for a and b, respectively. You substitute for a and b on the right hand side and show you can now derive the left hand side. Note that r_a is $a \ mod \ n$ and r_b is $b \ mod \ n$.

For **arithmetic modulo n**, let Z_n denote the set

$$Z_n = \{0, 1, 2, 3, \ldots.., n-1\}$$

Z_n is obviously **the set of remainders** in arithmetic modulo n. It is officially called the **set of residues**.

THE SET Z_n AND ITS PROPERTIES

The elements of Z_n obey the following properties:

Commutativity:

$$\begin{aligned} (w + x) \, mod \, n &= (x + w) \, mod \, n \\ (w \times x) \, mod \, n &= (x \times w) \, mod \, n \end{aligned}$$

Associativity:

$$\begin{aligned} [(w + x) + y] \, mod \, n &= [w + (x + y)] \, mod \, n \\ [(w \times x) \times y] \, mod \, n &= [w \times (x \times y)] \, mod \, n \end{aligned}$$

Distributivity of Multiplication over Addition:

$$[w \times (x + y)] \, mod \, n = [(w \times x) + (w \times y)] \, mod \, n$$

Existence of Identity Elements:

$$
\begin{aligned}
(0\ +\ w)\ mod\ n &= (w\ +\ 0)\ mod\ n \\
(1\ \times\ w)\ mod\ n &= (w\ \times\ 1)\ mod\ n
\end{aligned}
$$

Existence of Additive Inverses:

For each $w \in Z_n$, there exists a $z \in Z_n$ such that

$$w\ +\ z = 0\ mod\ n$$

Multiplicative Inverse:

For $w \in Z_n$, **IF** there exists an element $z \in Z_n$ such that

$$w \times z \equiv 1 \mod n$$

then z is the multiplicative inverse of w in Z_n.

Asymmetries Between Modulo Addition and Modulo Multiplication Over Z_n

For every element of Z_n, there exists an **additive inverse** in Z_n. But there does not exist a **multiplicative inverse** for every non-zero element of Z_n.

Shown below are the additive and the multiplicative inverses for **modulo 8** arithmetic:

Z_8	:	0	1	2	3	4	5	6	7
additive inverse	:	0	7	6	5	4	3	2	1
multiplicative inverse	:	-	1	-	3	-	5	-	7

Note that the **multiplicative inverses** exist for only those elements of Z_n that are **relatively prime** to n. Two integers are relatively prime to each other if the integer 1 is their only common positive divisor. More formally, two integers a and b are relatively prime to each other if $gcd(a, b) = 1$ where gcd denotes the **Greatest Common Divisor**.

The elements of Z_n that have a multiplicative inverse are called "units", the set if these "units" are denoted Z_n^*. For example $Z_6^* = \{1, 5\}$ and $Z_8^* = \{1, 3, 5, 7\}$.

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$\cdot$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

TABLE 3.3.2. Operational tables for $\mathbb{Z}_6$

The following property of **modulo n addition** is the same as for ordinary addition:

$$(a + b) \equiv (a + c) \; (mod \; n) \qquad implies \qquad b \equiv c \; (mod \; n)$$

But a similar property is **NOT** obeyed by **modulo n multiplication**. That is

$$(a \times b) \equiv (a \times c) \; (mod \; n) \qquad does \; not \; imply \qquad b \equiv c \; (mod \; n)$$

unless a and n are **relatively prime** to each other.

That the **modulo n addition** property stated above should hold true for all elements of Z_n follows from the fact that the **additive inverse** $-a$ exists for every $a \in Z_n$. So we can add $-a$ to both sides of the equation to prove the result.

To prove the same result for **modulo n multiplication**, we will need to multiply both sides of the second equation above by the multiplicative inverse a^{-1}. But, as you already know, not all elements of Z_n possess multiplicative inverses.

Since the existence of the multiplicative inverse for an element a of Z_n is predicated on a being **relatively prime** to n and since the answer to the question whether two integers are relatively prime to each other depends on their **greatest common divisor** (GCD), let's explore next the world's most famous algorithm for finding the GCD of two integers.

Euclid's Method for Finding the Greatest Common Divisor of Two Integers

We will now address the question of how to efficiently find the GCD of any two integers. [When there is a need to find the GCD of two integers in actual computer security algorithms, the two integers are always extremely large — much too large for human comprehension, as you will see in the lectures that follow.]

Euclid's algorithm for GCD calculation is based on the following observations

– $gcd(\ a,\ a) \ = \ a$

– $if\ \ b|a\ \ then\ \ gcd(\ a,\ b) \ = \ b$

– $gcd(\ a,\ 0) \ = \ a \quad since\ it\ is\ always\ true\ that\ \ a|0$

– Assuming without loss of generality that a is larger than b, it can be shown that

$$gcd(\ a,\ b) \quad = \quad gcd(\ b,\ a\ mod\ b\ )$$

The critical thing to note in the above recursion is that the right hand side of the equation is an easier problem to solve than the left hand side. While the largest number on the left is a, the largest number on the right is b, which is smaller than a.

Example: Euclid's Algortithm

$$\text{Find GCD}(70,38)$$

$$70 = 1(38) + 32$$

$$38 = 1(32) + 6$$

$$32 = 5(6) + 2$$

$$6 = 3(2) + 0$$

$$\Rightarrow \text{GCD}(70,38) = 2$$

Example: Euclid's Algorithm

Find the GCD(568,208):

$$568 = 2(208) + 152$$

$$208 = 1(152) + 56$$

$$152 = 2(56) + 40$$

$$56 = 1(40) + 16$$

$$40 = 2(16) + 8$$

$$16 = 2(8) + 0$$

$$\Rightarrow GCD(208,568) = 8$$

<u>Example: Euclid's Algorithm</u> (for relatively prime pair of integers)

$$\text{Find}\ \mathrm{GCD}(8,17)$$

$$17 = 2(8) + 1$$

$$8 = 8(1) + 0$$

$$\Rightarrow \mathrm{GCD}(8,17) = 1$$

Example: Euclid's Algorithm

$$\text{Find GCD}(40902, 24140)$$

Find GCD(40902,24140)

$$40902 = 1(24140) + 16762$$

$$24140 = 1(16762) + 7378$$

$$16762 = 2(7378) + 2006$$

$$7378 = 3(2006) + 1360$$

$$2006 = 1(1360) + 646$$

$$1360 = 2(646) + 68$$

$$646 = 9(68) + 34$$

$$68 = 2(34) + 0$$

$$\Rightarrow GCD(40902,\ 24140) = 34$$

Extended Euclidean Algorithm

Euclid's algorithm can be rearranged in such as way so as to enable us to find integers *m* and *n* such that

$$\boxed{\underline{\mathbf{GCD(a, b)}=\boldsymbol{m}\mathbf{a}+\boldsymbol{n}\mathbf{b}}}$$

Finding m and n is called the Extended Euclidean Algorithm.

This is a really useful application which is used in cryptography.

To find the integers *m* and *n*, we calculate the GCD as usual and then work backwards.

Example: Extended Euclidean Algorithm

$$\text{Find GCD}(8,17)$$

$$17 = 2(8)+1$$

$$8 = 8(1)+0$$

$$\Rightarrow \text{GCD}(8,17)=1$$

$$1 = 17 - 2(8)\text{....rearranging the line which has 1 as remainder}$$

$$\Rightarrow 1 = \mathbf{1}(17)-2(8)$$

$$\text{Therefore GCD}(8,17) = -2(8)+1(17)$$

$$\text{so } m = -2 \text{ and } n = 1$$

Back to Modular Arithmetic….

Given an element $[a]$ in $\mathbb{Z}_m^*$, its inverse can be computed by using the Euclidean algorithm to find $\gcd(a, m)$, since that algorithm also provides a solution to the equation $ax + my = \gcd(a, m) = 1$, which is equivalent to $ax \equiv 1 \pmod{m}$.

Example:

Use the Extended Euclidean Algorithm to find integers m and n such that

$$\text{GCD}(64, 17) = m(64) + n(17)$$

In other words, find the multiplicative inverse of 17 mod 64, $\mathbf{Z}_{64}^{*}$ **.**

Soln :

Part 1 :

$$64 = 3(17)+13$$

$$17 = 1(13)+4$$

$$13 = 3(4)+1$$

$$4 = 4(1)+0$$

Part II:

Working backwards

$$1 = 13 - 3(4)$$

$$1 = 13 - 3[17 - 1(13)]$$

$$= \mathbf{1}(13) - 3(17) + 3(13) = 4(13) - 3(17)$$

$$1 = 4[64 - 3(17)] - 3(17)$$

$$= 4(64) - 12(17) - 3(17) = 4(64) - 15(17)$$

$$\Rightarrow \quad \mathrm{GCD}(64, 17) = 1 = 4(64) - 15(17)$$

So $m = 4$ and $n = -15$.

However remember that in $\mathbf{Z}_{64}$ all integers must be between $\{0,1....63\}$ and so $-15 \notin \mathbf{Z}_{64}$.

To rectify this, we add 64 (or a multiple of 64) to -15 so that it becomes an integer between $\{0,1....63\}$.

$\Rightarrow -15 + 64 = 49$

So $m = 4$ and $n = 49$.

So the inverse of 17 in $\mathbf{Z}_{64}^{*}$ is 49.

$17^{-1} = 49 \pmod{64}$ or $17^{-1} \bmod 64 = 49$

Introduction to Diophantine Equations

The integer (whole) numbers are: 1,2,3,4, ...(positive integers) and also -1,-2,-3,... (negative integers).

When two or more integers are multiplied together to form a product, the numbers are called factors of that product.

For example, $2 \times 7 = 14$. The numbers 2 and 7 are the factors while 14 is the product.

Any integer has at least two factors (namely 1 and itself). Some integers have **only** 1 and itself as factors. These are called **prime** numbers. For example: $13 = 1 \times 13$.

Other integers have more than two factors. These are called composite numbers. For example: $24 = 1 \times 24 = 4 \times 6 = 3 \times 8$

Relatively prime Integers:

Two integers a and b are said to be relatively prime or coprime if

$$\gcd(a,b) = 1$$

So if a, b are relatively prime, then ∃ x, y integers such that

$$ax + by = 1$$

Example:

– 8 and 9 are relatively prime because gcd(8,9)=1.

– 3 and 9 are not relatively prime because gcd(8,9)≠1.

Prime Factorisation

To factorize an integer means to write it as the product of prime factors (that is, factors that cannot be factorized further). This factorisation is then unique.

Example

$$231 = 3 \times 7 \times 11; \qquad 200 = 2 \times 2 \times 3 \times 5 \times 5$$

☞ $\boxed{\text{\textbf{(Fundamental theorem of arithmetic)} Every integer can be uniquely written as the product of prime factors}}$

Example: Factorise the following integers, n, as the product of primes:

- **100**
- **54**
- **23**

Solution: Test which primes divide n, until all factors are prime.

- $100 = 2*2*5*5 = 2^2 \times 5^2$
- $54 = 2*27 = 2*3*3*3 = 2 \times 3^3$
- 23 = 23It is already prime, only factors are 1 and 23

Exercise:

Factorise the following integers as the product of primes:

- 1000
- 420
- 126
- 437
- 1039500

Linear Diophantine Equations

A **Diophantine Equation** is an equation whose roots are required to be integers.

i.e. A Diophantine equation is an equation of the form $ax + by = \gcd(a,b)$, for x, y integers .

Using the Extended Euclidean Algorithm we will find a *particular* solution to a Diophantine equation.

Note: Equations which have the form

$$ax+by=c$$

have a solution if and only if

gcd(a,b) divides c.

- Diophantine equations can also have more than one solution.

- If d = gcd(a,b), then the general solution is:

$$x_k = x + k(b/d) \qquad k \in \text{ integer},$$
$$y_k = y - k(a/d).$$

Example:

$5x + 3y = 1$ has solution $(x_0,y_0) = (-1,2)$.

This is called a *particular solution* because there are many more solutions that will work here.

More solutions to this equation can be found by adding any solution of the equation $5x + 3y = 0$ to the particular solution $(x_0,y_0) = (-1,2)$.

To illustrate: A solution to $5x + 3y = 0$ is $(x,y)=(3,-5)$.

Thus a *general solution* to the equation $5x + 3y = 1$ if given by

$$x_k = -1 + 3k$$

$$y_k = 2 - 5k \quad \text{for any } k \in Z$$

Diophantine Equations

Proposition 1:

Let a and b integers <> 0, with $d = \gcd(a,b)$.

If $d|c$, the solutions x and y of $ax + by = c$ are

$$x = x_0 + kb/d,$$

$$y = y_0 - ka/d \qquad \text{k an integer.}$$

where (x_0,y_0) is a particular solution.

If d does not divide c, there are no integer solutions.

Example 1. Consider the equation:

$$12x + 27y = 32$$

Since 3 = gcd(12,27) and 3 doesn't divide 32, it has no integer solutions for x and y.

Example 2. Consider the equation:

$$12x + 27y = 30$$

Since 3 = gcd(12, 27) and 3 divides 30, this equation has infinitely many integer solutions!

One solution is $x = -20$, $y = 10$.

Exercise. Find some more solutions, or them all.

Solution:

To find more solutions to the Diophantine equation $12x + 27y = 30$, we must first find integers x and y such that

$$12x + 27y = \gcd(12,27)=3$$

Using the Extended Euclidean Algorithm, we find that $x = -2,\ y = 1.$

Thus $$12(-2) +27(1) = 3$$

If we multiply this by 10, we get

$$12(-20) + 27(10) = 30$$

which is a particular solution i.e. $x = -20,\ y = 10.$

To find all of the solutions to the equation

$$12x + 27y = 30$$

we can use Proposition 1 from above.

Therefore, all of the solutions are given by:

$x = -20 + 27k/3$

Therefore $x = -20 + 9k$

$y = 10 – 12k/3$

Therefore $y = 10 – 4k$ $\forall$ integers k

Example:

Real-world applications. You have €4.27. Apples sell for 35 cents, and oranges for 49 cents.

What combination of apples and oranges will exhaust all your money?

Need to find integer solutions for

$$35x + 49y = 427.$$

---

1. Find gcd(35,49) and check it divides 427.
2. Use Extended Euclidean Algorithm to find particular solution for x and y.
3. Use Proposition 1 to find general(all) solutions for x and y.

Solution:

1. Firstly we will find gcd(35,49):

   $$49 = 1(35)+14$$

   $$35 = 2(14)+7$$

   $$14 = 2(7)+0$$

   So gcd(35, 49) = 7

   Since 7 divides 427 there are infinitely many solutions to the equation $35x + 49y = 427$.

2. Next we find integers x and y such that

$$35x + 49y = \gcd(35, 49) = 7$$

Using the Extended Euclidean Algorithm we get

$$\begin{aligned} 7 &= 35 - 2(14) \\ &= 35 - 2[49 - 1(35)] \\ &= 1(35) - 2(49) + 2(35) \end{aligned}$$

$\rightarrow \quad 7 = 3(35) - 2(49)$

So $x = 3$ and $y = -2$

Thus $35(3) + 49(-2) = 7$

- » Multiply this answer by 61 (to give 427)

Thus $35(183) + 49(-122) = 427$

$\rightarrow$ A *particular solution* is $x = 183$ and $y = -122$.

3. Using Proposition 1 we can get a *general solution:*

$$x = 183 + 49k/7$$

$\rightarrow$ $x = 183 + 7k$

$$y = -122 - 35k/7$$

$\rightarrow$ $y = -122 - 5k$

Exercises. Find all integer solutions of the following Diophantine equations if they exist.

- $42x + 30y = 20$
- $42x + 30y = 18$