MA294 Lecture

Timothy Kohl

Boston University

July 1, 2025

Recall that if $a \in \mathbb{Z}_m$ there exist $b \in \mathbb{Z}_m$ such that $a + b = 0$, i.e. $b = -a$.

For the multiplication operation, the analogue would be:

$$\text{For each } a \in \mathbb{Z}_m \text{ there exists } b \in \mathbb{Z}_m \text{ such that } a \cdot b = 1$$

The problem is that this is not always the case.

For example, in $\mathbb{Z}_6$, if $a = 2$ then $b \in \mathbb{Z}_6$ would have to have the property that $2b \equiv 1 \ (mod\ 6)$, but observe that for $\mathbb{Z}_6$ we have

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

So $2b = 1$ is impossible.

However, depending on the modulus m and $a \in \mathbb{Z}_m$ one does have such 'multiplicative inverses'.

Example: In $\mathbb{Z}_9 = \{0,1,2,3,4,5,6,7,8\}$ let $a = 2$ then one may verify that $b = 5$ is such that $ab = 1$, i.e. $2 \cdot 5 = 10 = 1$ in $\mathbb{Z}_9$, i.e. We may write $2^{-1} = 5$ in $\mathbb{Z}_9$.

Definition

An element $r \in \mathbb{Z}_m$ is invertible (or a unit mod m) if there is some $x \in \mathbb{Z}_m$ such that $rx = 1$ in $\mathbb{Z}_m$.
In that case, x is called the multiplicative inverse of r and we write $r^{-1} = x$.

Example: Again in $\mathbb{Z}_9$, $4^{-1} = 7$ since $4 \cdot 7 = 28 \equiv 1 \ (mod\ 9)$.

Note, in contrast, that 6^{-1} does not exist in $\mathbb{Z}_9$.Why?

Theorem

The only $r \in \mathbb{Z}_m$ that have inverses are those for which $gcd(r, m) = 1$, that is 'r is co-prime to m'.

Recall that $gcd(r, m)$ means 'greatest common divisor of r and m'.

Proof.

Suppose $rx = 1$ in $\mathbb{Z}_m$ then we have

$$rx - 1 = qm$$

for some q.

Well then $rx - qm = 1$ so if $d|r$ and $d|m$ (i.e. d divides r and m) then $r = da$ for some a, and $m = db$ for some b.

But then $rx - qm = dax - qdb = d(ax - qb)$ but $rx - qm = 1$ do that $d|1$!

So the only conclusion is that $d = 1$, i.e. the only common divisor of r and m is 1. For the converse we use the following FACT known as *Bezout's Identity* which is that, if $gcd(r, m) = 1$ then there exists a, b such that $ar + bm = 1$.

As such, $ar - 1 = (-b)m$ which means $ar \equiv 1 \ (mod\ m)$ i.e. $r^{-1} = a$, that is, r is invertible. □

The invertible elements of $\mathbb{Z}_m$ gives rise to this.

Definition

For $m > 1$ the <u>units mod m</u> is

$$U(m) = \{r \in \mathbb{Z}_m \, | gcd(r, m) = 1\}$$

which is precisely the set of invertible elements of $\mathbb{Z}_m$.

Note, $0 \notin U(m)$ for any m and the size of $U(m)$ (as a set) is what is known as

$$\phi(m) = \text{ Euler's Function, or Totient}$$

and it is interesting to consider the value of $\phi(m)$.

Example:

- $\mathbb{Z}_2 = \{0,1\} \to U(2) = \{1\} \to \phi(2) = 1$
- $\mathbb{Z}_3 = \{0,1,2\} \to U(3) = \{1,2\} \to \phi(3) = 2$
- $\mathbb{Z}_4 = \{0,1,2,3\} \to U(4) = \{1,3\} \to \phi(4) = 2$
- $\mathbb{Z}_5 = \{0,1,2,3,4\} \to U(5) = \{1,2,3,4\} \to \phi(5) = 4$
- $\mathbb{Z}_6 = \{0,1,2,3,4,5\} \to U(6) = \{1,5\} \to \phi(6) = 2$
- $\mathbb{Z}_7 = \{0,1,2,3,4,5,6\} \to U(7) = \{1,2,3,4,5,6\} \to \phi(7) = 6$
- $\mathbb{Z}_8 = \{0,1,2,3,4,5,6,7\} \to U(8) = \{1,3,5,7\} \to \phi(8) = 4$
- $\mathbb{Z}_9 = \{0,1,2,3,4,5,6,7,8\} \to U(9) = \{1,2,4,5,7,8\} \to \phi(9) = 6$

One observation we can make about the ϕ function is that if m is prime then $\phi(m) = m - 1$.

The reason for this is that if m is prime then any $r < m$ is never a divisor since m is prime.

But before developing further properties of ϕ we need some to make some observations about $U(m)$.

- If $r, s \in U(m)$ then $rs \in U(m)$.(Why? Well $gcd(r, m) = 1$ and $gcd(s, m) = 1$ implies $gcd(rs, m) = 1$.)
- $1 \in U(m)$ for all m (obviously, since $1 \cdot 1 = 1$ so $1^{-1} = 1$)
- If $r \in U(m)$ then $r^{-1} \in U(m)$.[Exercise]

These properties, as we'll discuss later on, make $U(m)$ into what we know as a *group*.

One important property of ϕ is this.

Proposition

If $gcd(r,s) = 1$ then $\phi(rs) = \phi(r)\phi(s)$.

Proof.

(Sketch)The basic idea is to consider the function $\rho : U(rs) \rightarrow U(r) \times U(s)$ defined by $\rho(x) = (x^*, x^{**})$ where x^* is the remainder when x is divided by r and x^{**} is the remainder when x is divided by s.

As $gcd(r,s) = 1$ then one can show that this map is 1-1 and onto, so that

$$|U(rs)| = |U(r) \times U(s)| = |U(r)| \cdot |U(s)|$$

namely that $\phi(rs) = \phi(r)\phi(s)$. □

We should note that this not necessarily true if r and s are not relatively prime.

We have another very important property of the ϕ function, in particular to its application to modern cryptography.

Theorem

If $a \in U(m)$ then $a^{\phi(m)} \equiv 1 \pmod{m}$. (Euler - 1763)

Proof.

(Sketch) If $U(m) = \{a_1, a_2, \ldots, a_{\phi(m)}\}$ where, without loss of generality $a_1 = 1$ then for $a \in U(m)$ consider

$$\{aa_1, aa_2, \ldots, aa_{\phi(m)}\}$$

and observe that, since $a \in U(m)$ then $aa_i = aa_j$ implies $a^{-1}aa_i = a^{-1}aa_j$, that is $(a^{-1}a)a_i = (a^{-1}a)a_j$ and since $a^{-1}a = 1$ then this implies that $a_i = a_j$. As such, $\{aa_1, aa_2, \ldots, aa_{\phi(m)}\}$ is a rearrangement (or permutation) of $\{a_1, a_2, \ldots, a_{\phi(m)}\}$ and so

$$aa_1 aa_2 \ldots aa_{\phi(m)} = a_1 a_2 \cdots a_{\phi(m)}$$

namely $a^{\phi(m)} b = b$ where $b = (a_1 a_2 \cdots a_{\phi(m)})$ which means

$$a^{\phi(m)} bb^{-1} = bb^{-1}$$

where, of course $bb^{-1} = 1$ so $a^{\phi(m)} = 1$. □

A simpler version of this result is known as Fermat's (Little) Theorem, namely for $m = p$ a prime and $gcd(a, p) = 1$ then $a^{p-1} \equiv 1 \ (mod \ p)$ since $\phi(p) = p - 1$.

As mentioned earlier, Euler's theorem (although a 200+ year old theorem) is at the heart of the RSA (public key) encryption system that is integral to modern electronic commerce and general security online.

RSA Encryption

For a modulus $m > 1$ we showed for $a \in U(m)$ that $a^{\phi(m)} \equiv 1 \ (mod\ \ m)$. A simple consequence of this is obtained if we multiply both sides by a, namely that

$$a^{\phi(m)+1} \equiv a \ (mod\ \ m)$$

and, in fact, this theorem is true even if $a \in \mathbb{Z}_m$ and not just in $U(m)$, which is particularly useful in its application to cryptography.

One of the other preparatory points to note/recall is that $\phi(rs) = \phi(r)\phi(s)$ if $gcd(r, s) = 1$, and in particular, if p and q are distinct primes, then certainly $gcd(p, q) = 1$ and so $\phi(pq) = \phi(p)\phi(q) = (p - 1)(q - 1)$.

The other operational fact, which is also at the heart of the security of the RSA algorithm we'll present, is that while it's easy to multiply two large numbers, it is computationally quite difficult to take a large number and find its constituent factors.

So, in particular, if p and q are 'large' primes then $m = pq$ is an even larger number, and if one were given such a large number without knowing 'p' and 'q' then it would be quite difficult to factor m to find p and q.

Indeed, it is the relatively difficulty of factorization, as we'll see, which is what makes the RSA algorithm secure.

And this also touches on the subject of 'quantum computers' (outside the scope of this course) which are basically computer systems for which factorization is feasible in a 'reasonable' amount of time, as compared with the 'ordinary' computers of today.

The one saving factor though, is that these quantum computers are extremely difficult to build and work with, and it is generally accepted that they haven't been used for this purpose...yet!

RSA Encryption

- Let $m = pq$ where p,q are 'big' primes. (Keep p,q secret.)
- Choose k such that $gcd(k, \phi(m)) = 1$.
- Find 'j' such that $kj \equiv 1 \ (mod \ \phi(m))$, i.e. $kj = t\phi(m) + 1$ (keep j secret!)
- Publish k and m. (This is the 'public' part of public-key encryption.)
- If a sender has a message, representable as a number a, where presumably $a < m$ then they compute a^k mod m which is the encrypted message they transmit.
- The recepient then takes a^k and computes $(a^k)^j$.

The end result is that

$$\begin{aligned} a^{kj} = a^{t\phi(m)+1} &= (a^{\phi(m)})^t a \\ &\equiv 1 \cdot a \ (mod \ \ m) \\ &\equiv a \ (mod \ \ m) \end{aligned}$$

So the recepient now has the message the sender wanted to transmit, the number a.

For a bit of history, the earliest versions used numbers $m = pq$ of around 100 digits which is about 330 binary digits.

[Indeed sometimes these numbers are given in units of how long they are in binary digits.]

And there was a challenge early on posed by the developers (R.S.A.) to see who could factor some large numbers, and as time passed, and techniques and computing power increased, the bit length had to be increased to continue the challenge.

There are many resources online describing this, which one may readily find.

Latin Squares

Consider $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ and all the possible $i + j$ for $i, j \in \mathbb{Z}_4$.

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

where we emphasize how the table entries in the 'inner' 4×4 square are filled in, based on adding the entries in the row and side column, e.g. $1 + 2 = 3$.

If we remove the top row, and left column we get the table:

0	1	2	3
1	2	3	0
2	3	0	1
3	0	1	2

and we observe the most important feature, namely that each row and each column contains exactly one element from $\{0, 1, 2, 3\}$ with no repeats.

What does this remind you of?

Definition

A latin square of order n is an $n \times n$ array in which each one of n symbols occurs once in each row and once in each column.

A more interesting example, for $n = 6$.

A	B	C	D	E	F
B	A	E	F	C	D
C	F	A	E	D	B
D	E	F	A	B	C
E	D	B	C	F	A
F	C	D	B	A	E

For a latin square L one may define $L(i,j)$ to mean the entry at the i-th row and j-th column.

So for above we have $L(2,3) = E$, $L(4,6) = C$ and we can fram the latin square condition in terms of the $L(i,j)$.

Namely L is a latin square iff $L(i,j) = L(i,k)$ only if $j = k$ and $L(i,j) = L(k,j)$ only if $i = k$.

Going back to the example with $\mathbb{Z}_4$ earlier, we have the following general statement.

Theorem

For each $m > 1$ the $m \times m$ array defined by $L(i,j) = i + j$ for $i, j \in \mathbb{Z}_m$ is a latin square.

Proof.

If $L(i,j) = L(i,k)$ then $i + j = i + k$, so can we conclude $j = k$ in $\mathbb{Z}_m$? Well, in $\mathbb{Z}_m$, every element as an additive inverse, so in particular

$$\begin{aligned} i + j &= i + k \\ (-i) + i + j &= (-i) + i + k \\ 0 + j &= 0 + k \\ j &= k \end{aligned}$$

and similarly $L(i,j) = L(k,j)$ implies $i = k$. □

So what this shows is that for *every* m there is an $m \times m$ latin square.

However, there are other examples as our 6×6 example earlier demonstrates, but even for 4×4 we can find another (actually natural) example.

A	B	C	D
B	A	D	C
C	D	A	B
D	C	B	A

as compared with the $\mathbb{Z}_4$ example (expressed with letters instead of numbers)

A	B	C	D
B	C	D	A
C	D	A	B
D	A	B	C

Before going further we should point out that latin squares have a number of different applications.

One of these is in experimental design.

Suppose you have four test subjects, each of which is questioned separately by four interviewers over four rounds of questioning, and you want to make sure every interviewer interviews one and only one test subject, but that every interviewer interviews every subject.

If the four interviewers are $\{1, 2, 3, 4\}$ and the subjects are A, B, C, D and the 'rounds' $R1, R2, R3, R4$ then a latin square can be used to distribute the subjects between the interviewers in each round.

	1	2	3	4
$R1$	A	B	C	D
$R2$	B	C	D	A
$R3$	C	D	A	B
$R4$	D	A	B	C

This is a fairly obvious plan since the 'cyclic' rotation of subjects A,B,C,D, amongst the interviewers obviously guarntees that the conditions of the experiment are satisfied.

An alternate choice is the other one we saw above.

	1	2	3	4
$R1$	A	B	C	D
$R2$	B	A	D	C
$R3$	C	D	A	B
$R4$	D	C	B	A

A natural question is how many latin squares are there of a given size $n \times n$?

The first observation one can make which helps streamline the discussion is that for any latin square in the set $S = \{x_1, \ldots, x_n\}$, one may assume that the first row and the first column are in the same order. i.e.

x_1	x_2	$\ldots$	x_n
x_2	$\ddots$		
$\vdots$			
x_n			

and such latin squares are called reduced.

The number of (reduced) latin squares for small n can be determined:
$n = 1 \rightarrow 1$

$n = 2 \rightarrow 1$ (If the first row and column are given, there is only one way to fill in the remaing cell!)

$n = 3 \rightarrow 1$

A	B	C
B	?	?
C	?	?

$n = 4 \rightarrow 2$ (the ones we've seen already, and no others)
$n = 5 \rightarrow 56$ (This is not a typo!)
$n = 6 \rightarrow 9408$ (This is also not a typo!)
$n = 7 \rightarrow 16,942,080$ (Also not a typo.)

You get the idea.