IN MY PAPER, I USE AN EXTENSION OF THE DIVISOR FUNCTION OVER THE GAUSSIAN INTEGERS TO GENERALIZE THE SO-CALLED "FRIENDLY NUMBERS" INTO THE COMPLEX PLANE.

HOLD ON, IS THIS PAPER SIMPLY A GIANT BUILD-UP TO AN "IMAGINARY FRIENDS" FUN?

IT MIGHT NOT BE.

I'M SORRY, WE'RE REVOKING YOUR MATH LICENSE.
## Divisibility

**Definition: “a divides b”**

For $a \in \mathbb{Z}$, $b \in \mathbb{Z}$ with $a \neq 0$:

$$a \mid b \iff \exists k \in \mathbb{Z} \ (b = ka)$$

---

Check Your Understanding. Which of the following are true?

<table>
<thead>
<tr>
<th>$a$</th>
<th>$b$</th>
<th>Condition</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>1</td>
<td>$5 \mid 1 \iff 1 = 5k$</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>$25 \mid 5 \iff 5 = 25k$</td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td>$5 \mid 0 \iff 0 = 5k$</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>$3 \mid 2 \iff 2 = 3k$</td>
</tr>
<tr>
<td>1</td>
<td>5</td>
<td>$1 \mid 5 \iff 5 = 1k$</td>
</tr>
<tr>
<td>5</td>
<td>25</td>
<td>$5 \mid 25 \iff 25 = 5k$</td>
</tr>
<tr>
<td>0</td>
<td>5</td>
<td>$0 \mid 5 \iff 5 = 0k$</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
<td>$2 \mid 3 \iff 3 = 2k$</td>
</tr>
</tbody>
</table>
Division Theorem

For $a \in \mathbb{Z}$, $d \in \mathbb{Z}$ with $d > 0$
there exist unique integers $q, r$ with $0 \leq r < d$
such that $a = dq + r$.

To put it another way, if we divide $d$ into $a$, we get a
unique quotient $q = a \text{ div } d$
and non-negative remainder $r = a \text{ mod } d$

Note: $r \geq 0$ even if $a < 0$.
Not quite the same as $a \% d$. 

Division Theorem

For \( a \in \mathbb{Z}, d \in \mathbb{Z} \) with \( d > 0 \)
there exist unique integers \( q, r \) with \( 0 \leq r < d \)
such that \( a = dq + r \).

To put it another way, if we divide \( d \) into \( a \), we get a unique quotient
\[ q = a \div d \]
and non-negative remainder
\[ r = a \mod d \]

public class Test2 {
    public static void main(String args[]) {
        int a = -5;
        int d = 2;
        System.out.println(a % d);
    }
}

Note: \( r \geq 0 \) even if \( a < 0 \).
Not quite the same as \( a \% d \).
Arithmetic, mod 7

\[a +_7 b = (a + b) \mod 7\]
\[a \times_7 b = (a \times b) \mod 7\]
Modular Arithmetic

<table>
<thead>
<tr>
<th>Definition: “a is congruent to b modulo m”</th>
</tr>
</thead>
<tbody>
<tr>
<td>For $a, b, m \in \mathbb{Z}$ with $m &gt; 0$</td>
</tr>
<tr>
<td>$a \equiv b \pmod{m} \iff m \mid (a - b)$</td>
</tr>
</tbody>
</table>

Check Your Understanding. What do each of these mean? When are they true?

- $x \equiv 0 \pmod{2}$  
  $x$ is even

- $-1 \equiv 19 \pmod{5}$  
  true

- $y \equiv 2 \pmod{7}$  
  the set of form $2 + 7\mathbb{Z}$: $-5, 2, 9, 16, \ldots$
Modular Arithmetic

Definition: “a is congruent to b modulo m”
For $a, b, m \in \mathbb{Z}$ with $m > 0$
\[ a \equiv b \pmod{m} \iff m \mid (a - b) \]

Check Your Understanding. What do each of these mean? When are they true?

$x \equiv 0 \pmod{2}$
This statement is the same as saying “x is even”; so, any x that is even (including negative even numbers) will work.

$-1 \equiv 19 \pmod{5}$
This statement is true. $19 - (-1) = 20$ which is divisible by 5

$y \equiv 2 \pmod{7}$
This statement is true for y in { ..., -12, -5, 2, 9, 16, ...}. In other words, all y of the form $2 + 7k$ for k an integer.
Let $a, b, m$ be integers with $m > 0$. Then, $a \equiv b \pmod{m}$ if and only if $a \mod m = b \mod m$.

Suppose that $a \equiv b \pmod{m}$.

\[
\begin{align*}
\text{By Division Theorem } & \quad \text{for some integer } q, s, r \quad 0 \leq r < m \\
& \quad a = bq + r \quad b = qm + r \\
& \quad a \mod m = r \quad a \mod m = r \mod m
\end{align*}
\]

Suppose that $a \mod m = b \mod m$.

\[
\begin{align*}
& \quad \text{for some integer } q, s, r \quad 0 \leq r < m \\
& \quad b = sqm + r \\
& \quad a - b = (q-s)m \\
& \quad \therefore \quad m \mid (a-b) \quad \therefore \quad a \equiv b \pmod{m}
\end{align*}
\]
**Modular Arithmetic: A Property**

Let $a, b, m$ be integers with $m > 0$.

Then, $a \equiv b \pmod{m}$ if and only if $a \mod m = b \mod m$.

Suppose that $a \equiv b \pmod{m}$.

Then, $m \mid (a - b)$ by definition of congruence.

So, $a - b = km$ for some integer $k$ by definition of divides.

Therefore, $a = b + km$.

Taking both sides modulo $m$ we get:

$$a \mod m = (b + km) \mod m \equiv b \mod m.$$ 

Suppose that $a \mod m = b \mod m$.

By the division theorem, $a = mq + (a \mod m)$ and

$$b = ms + (b \mod m)$$

for some integers $q,s$.

Then, $a - b = (mq + (a \mod m)) - (ms + (b \mod m))$

$$= m(q - s) + (a \mod m - b \mod m)$$

$$= m(q - s)$$

since $a \mod m = b \mod m$.

Therefore, $m \mid (a - b)$ and so $a \equiv b \pmod{m}$. 

The mod $m$ function vs the $\equiv (\text{mod } m)$ predicate

- What we have just shown
  - The mod $m$ function takes any $a \in \mathbb{Z}$ and maps it to a remainder $a \mod m \in \{0,1,\ldots,m-1\}$.
  
  - Imagine grouping together all integers that have the same value of the mod $m$ function
    That is, the same remainder in $\{0,1,\ldots,m-1\}$.

  - The $\equiv (\text{mod } m)$ predicate compares $a, b \in \mathbb{Z}$. It is true if and only if the mod $m$ function has the same value on $a$ and on $b$.
    That is, $a$ and $b$ are in the same group.
Modular Arithmetic: Addition Property

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

Proof: Suppose \( a \equiv b \pmod{m} \) and \( c \equiv d \pmod{m} \).

Then \( m \mid (a-b) \) and \( m \mid (c-d) \).

\[
\begin{align*}
    a - b &= km \\
    c - d &= sm
\end{align*}
\]

for some integers \( k \) and \( s \).

Then
\[
\begin{align*}
    a - b + c - d &= km + sm \\
    (a + c) - (b + d) &= km + sm
\end{align*}
\]

Thus
\[
\begin{align*}
    m \mid ((a+c)-(b+d))
\end{align*}
\]

\[
\begin{align*}
    a + c \equiv b + d \pmod{m}
\end{align*}
\]
Let $m$ be a positive integer. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a + c \equiv b + d \pmod{m}$.

Suppose that $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$. Unrolling definitions gives us some $k$ such that $a - b = km$, and some $j$ such that $c - d = jm$.

Adding the equations together gives us 

$$(a + c) - (b + d) = m(k + j).$$

Now, re-applying the definition of congruence gives us $a + c \equiv b + d \pmod{m}$. 
Modular Arithmetic: Multiplication Property

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

Proof: Suppose that \( a \equiv b \pmod{m} \) and \( c \equiv d \pmod{m} \).

\[ a - b = km \quad \text{for some integer } k \]
\[ c - d = sm \quad \text{for some integer } s. \]

\[ a = b + km \quad \text{and} \quad c = d + sm \]

\[ ac = (b + km)(d + sm) = bd + bs + km + ksm^2 \]
\[ = bd + m(bs + km + ksm) \] (integer)
\[ m \mid (ac - bd) \]
\[ \therefore \quad ac \equiv bd \pmod{m} \] (Q.E.D.)
Let $m$ be a positive integer. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $ac \equiv bd \pmod{m}$

Suppose that $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$. Unrolling definitions gives us some $k$ such that $a - b = km$, and some $j$ such that $c - d = jm$.

Then, $a = km + b$ and $c = jm + d$. Multiplying both together gives us $ac = (km + b)(jm + d) = k jm^2 + kmd + bjm + bd$.

Re-arranging gives us $ac - bd = m(kjm + kd + bj)$.
Using the definition of congruence gives us $ac \equiv bd \pmod{m}$.
Example

Let $n$ be an integer.
Prove that $n^2 \equiv 0 \pmod{4}$ or $n^2 \equiv 1 \pmod{4}$

Let’s start by looking at a small example:

- $0^2 = 0 \equiv 0 \pmod{4}$
- $1^2 = 1 \equiv 1 \pmod{4}$
- $2^2 = 4 \equiv 0 \pmod{4}$
- $3^2 = 9 \equiv 1 \pmod{4}$
- $4^2 = 16 \equiv 0 \pmod{4}$
Example

Let $n$ be an integer.
Prove that $n^2 \equiv 0 \pmod{4}$ or $n^2 \equiv 1 \pmod{4}$

Case 1 (n is even):

1. $n = 0 \pmod{2}$
2. $n = 2k$ for some integer $k$
3. $n^2 = 4k^2$
4. $n^2 \equiv 0 \pmod{4}$

Case 2 (n is odd):

1. $n \equiv 1 \pmod{2}$
2. $n = 2k+1$ for some integer $k$
3. $n^2 = (2k+1)^2$
4. $n^2 = 4k^2 + 4k + 1$
5. $n^2 \equiv 1 \pmod{4}$

Let’s start by looking at a small example:

- $0^2 = 0 \equiv 0 \pmod{4}$
- $1^2 = 1 \equiv 1 \pmod{4}$
- $2^2 = 4 \equiv 0 \pmod{4}$
- $3^2 = 9 \equiv 1 \pmod{4}$
- $4^2 = 16 \equiv 0 \pmod{4}$

It looks like

$n \equiv 0 \pmod{2} \rightarrow n^2 \equiv 0 \pmod{4}$, and
$n \equiv 1 \pmod{2} \rightarrow n^2 \equiv 1 \pmod{4}$. 
Example

Let $n$ be an integer. Prove that $n^2 \equiv 0 \pmod{4}$ or $n^2 \equiv 1 \pmod{4}$

Let’s start by looking at a small example:

<table>
<thead>
<tr>
<th>$n$</th>
<th>$n^2 \pmod{4}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
</tr>
</tbody>
</table>

It looks like $n \equiv 0 \pmod{2} \rightarrow n^2 \equiv 0 \pmod{4}$, and $n \equiv 1 \pmod{2} \rightarrow n^2 \equiv 1 \pmod{4}$.

Case 1 ($n$ is even):
Suppose $n \equiv 0 \pmod{2}$.
Then, $n = 2k$ for some integer $k$.
So, $n^2 = (2k)^2 = 4k^2$. So, by definition of congruence, $n^2 \equiv 0 \pmod{4}$.

Case 2 ($n$ is odd):
Suppose $n \equiv 1 \pmod{2}$.
Then, $n = 2k + 1$ for some integer $k$.
So, $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 4(k^2 + k) + 1$.
So, by definition of congruence, $n^2 \equiv 1 \pmod{4}$.
Represent integer $x$ as sum of powers of 2:

If $\sum_{i=0}^{n-1} b_i 2^i$ where each $b_i \in \{0, 1\}$

then representation is $b_{n-1}...b_2 b_1 b_0$

99 = 64 + 32 + 2 + 1
18 = 16 + 2

For n = 8:

99: 0110 0011
18: 0001 0010
Sign-Magnitude Integer Representation

$n$-bit signed integers
Suppose that $-2^{n-1} < x < 2^{n-1}$
First bit as the sign, $n - 1$ bits for the value

$99 = 64 + 32 + 2 + 1$
$18 = 16 + 2$

For $n = 8$:
- $99$: 0110 0011
- $-18$: 1001 0010

Any problems with this representation?
Two’s Complement Representation

\( n \) bit signed integers, first bit will still be the sign bit

Suppose that \( 0 \leq x < 2^{n-1} \),
\( x \) is represented by the binary representation of \( x \)

Suppose that \( 0 \leq x \leq 2^{n-1} \),
\( -x \) is represented by the binary representation of \( 2^n - x \)

**Key property:** Twos complement representation of any number \( y \)
is equivalent to \( y \mod 2^n \) so arithmetic works \( \mod 2^n \)

\[
\begin{align*}
99 &= 64 + 32 + 2 + 1 \\
18 &= 16 + 2 \\
\end{align*}
\]

For \( n = 8 \):
- 99: 0110 0011
- -18: 1110 1110
## Sign-Magnitude vs. Two’s Complement

<table>
<thead>
<tr>
<th></th>
<th>-7</th>
<th>-6</th>
<th>-5</th>
<th>-4</th>
<th>-3</th>
<th>-2</th>
<th>-1</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
</tr>
</thead>
<tbody>
<tr>
<td>SM</td>
<td>1111</td>
<td>1110</td>
<td>1101</td>
<td>1100</td>
<td>1011</td>
<td>1010</td>
<td>1001</td>
<td>0000</td>
<td>0001</td>
<td>0010</td>
<td>0011</td>
<td>0100</td>
<td>0101</td>
<td>0110</td>
<td>0111</td>
</tr>
<tr>
<td>TC</td>
<td>1000</td>
<td>1001</td>
<td>1010</td>
<td>1011</td>
<td>1100</td>
<td>1101</td>
<td>1110</td>
<td>1111</td>
<td>0000</td>
<td>0001</td>
<td>0010</td>
<td>0011</td>
<td>0100</td>
<td>0101</td>
<td>0110</td>
</tr>
</tbody>
</table>

Sign-bit

Two’s complement
Two’s Complement Representation

• For $0 < x \leq 2^{n-1}$, $-x$ is represented by the binary representation of $2^n - x$
  
  — That is, the two’s complement representation of any number $y$ has the same value as $y$ modulo $2^n$.

• To compute this: Flip the bits of $x$ then add 1:
  
  — All 1’s string is $2^n - 1$, so
  
  Flip the bits of $x \equiv$ replace $x$ by $2^n - 1 - x$
  
  Then add 1 to get $2^n - x$
Basic Applications of mod

- Hashing
- Pseudo random number generation
- Simple cipher
Hashing

Scenario:
Map a small number of data values from a large domain \( \{0, 1, \ldots, M - 1\} \) ...
...into a small set of locations \( \{0, 1, \ldots, n - 1\} \) so one can quickly check if some value is present

- \( \text{hash}(x) = x \mod p \) for \( p \) a prime close to \( n \)
  - or \( \text{hash}(x) = (ax + b) \mod p \)

- Depends on all of the bits of the data
  - helps avoid collisions due to similar values
  - need to manage them if they occur
Pseudo-Random Number Generation

Linear Congruential method

\[ x_{n+1} = (a \cdot x_n + c) \mod m \]

Choose random \( x_0, a, c, m \) and produce a long sequence of \( x_n \)'s
Simple Ciphers

- **Caesar cipher**, \( A = 1, B = 2, \ldots \)
  - HELLO WORLD

- **Shift cipher**
  - \( f(p) = (p + k) \mod 26 \)
  - \( f^{-1}(p) = (p - k) \mod 26 \)

- **More general**
  - \( f(p) = (ap + b) \mod 26 \)