Lecture 11: Modular Arithmetic, Applications and Factoring
## Last Class: 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>$5 \mid 1$</th>
<th>$25 \mid 5$</th>
<th>$5 \mid 0$</th>
<th>$3 \mid 2$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$5 \mid 1$ iff $1 = 5k$</td>
<td>$25 \mid 5$ iff $5 = 25k$</td>
<td>$5 \mid 0$ iff $0 = 5k$</td>
<td>$3 \mid 2$ iff $2 = 3k$</td>
</tr>
<tr>
<td>$1 \mid 5$</td>
<td>$5 \mid 25$</td>
<td>$0 \mid 5$</td>
<td>$2 \mid 3$</td>
</tr>
<tr>
<td>$1 \mid 5$ iff $5 = 1k$</td>
<td>$5 \mid 25$ iff $25 = 5k$</td>
<td>$0 \mid 5$ iff $5 = 0k$</td>
<td>$2 \mid 3$ iff $3 = 2k$</td>
</tr>
</tbody>
</table>
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 \( a \% d \).
Last Class: Arithmetic, mod 7

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

<table>
<thead>
<tr>
<th>+</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>6</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>6</td>
<td>6</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>×</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>2</td>
<td>4</td>
<td>6</td>
<td>1</td>
<td>3</td>
<td>5</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>3</td>
<td>6</td>
<td>2</td>
<td>5</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>4</td>
<td>1</td>
<td>5</td>
<td>2</td>
<td>6</td>
<td>3</td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td>5</td>
<td>3</td>
<td>1</td>
<td>6</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>6</td>
<td>0</td>
<td>6</td>
<td>5</td>
<td>4</td>
<td>3</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>
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.
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:
\[
a \mod m = (b + km) \mod m = b \mod m.
\]
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 \(a \equiv b \pmod{m}\).

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, \(a - b = (mq + (a \mod m)) - (ms + (b \mod m)) = m(q - s) + (a \mod m - b \mod m)\) since \(a \mod m = b \mod m\).

Therefore, \(m \mid (a - b)\) and so \(a \equiv b \pmod{m}\).
Last Class: $\mod m$ function vs $\equiv \pmod{m}$ 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 $\equiv \pmod{m}$ 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 $a + c \equiv b + d \pmod{m}$
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 \( ac \equiv bd \pmod{m} \).
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 $ac = (km + b)(jm + d) = km^2 + kmd + bjm + bd$.

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

**Modular Arithmetic: Multiplication Property**
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):

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

$n \equiv 1 \pmod{2} \rightarrow n^2 \equiv 1 \pmod{4}$.

Case 2 (n is odd):
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):
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, $n^2 \equiv 1 \pmod{4}$.

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
$n \equiv 1 \pmod{2} \rightarrow n^2 \equiv 1 \pmod{4}$. 

Let $/ \in \mathbb{Z}$ be an integer.
Prove that $/^0 \equiv 0 \pmod{2}$ or $/^0 \equiv 1 \pmod{2}$. 

n-bit Unsigned Integer Representation

• Represent integer $x$ as sum of powers of 2:

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

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

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 \( \mod 2^n \)

\[
99 = 64 + 32 + 2 + 1 \\
18 = 16 + 2
\]

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

<table>
<thead>
<tr>
<th></th>
<th>-8</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></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>
<td>0111</td>
</tr>
</tbody>
</table>

**Sign-bit**

<table>
<thead>
<tr>
<th></th>
<th>-8</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></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>
<td></td>
</tr>
</tbody>
</table>

**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

These applications work well because of how we can solve equations involving mods
  — To understand that we need a bit more number theory...
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

- \( \text{hash}(x) = (ax + b) \mod p \) for a prime \( p \)
  close to \( n \) and values \( a \) and \( b \)
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
  \[- f(p) = (ap + b) \mod 26 \]
Primality

An integer $p$ greater than 1 is called *prime* if the only positive factors of $p$ are 1 and $p$.

A positive integer that is greater than 1 and is not prime is called *composite*. 
Fundamental Theorem of Arithmetic

Every positive integer greater than 1 has a unique prime factorization

\[ 48 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 \]
\[ 591 = 3 \cdot 197 \]
\[ 45,523 = 45,523 \]
\[ 321,950 = 2 \cdot 5 \cdot 5 \cdot 47 \cdot 137 \]
\[ 1,234,567,890 = 2 \cdot 3 \cdot 3 \cdot 5 \cdot 3,607 \cdot 3,803 \]
Euclid’s Theorem

There are an infinite number of primes.

Proof by contradiction:

Suppose that there are only a finite number of primes and call the full list $p_1, p_2, \ldots, p_n$. 
Euclid’s Theorem

There are an infinite number of primes.

Proof by contradiction:

Suppose that there are only a finite number of primes and call the full list $p_1, p_2, \ldots, p_n$.

Define the number $P = p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_n$ and let $Q = P + 1$. 
Euclid’s Theorem

There are an infinite number of primes.

Proof by contradiction:

Suppose that there are only a finite number of primes and call the full list $p_1, p_2, \ldots, p_n$.

Define the number $P = p_1 \cdot p_2 \cdot p_3 \cdots p_n$ and let $Q = P + 1$.

Case 1: $Q$ is prime: Then $Q$ is a prime different from all of $p_1, p_2, \ldots, p_n$ since it is bigger than all of them.
Euclid’s Theorem

There are an infinite number of primes.

Proof by contradiction:

Suppose that there are only a finite number of primes and call the full list \( p_1, p_2, ..., p_n \).

Define the number \( P = p_1 \cdot p_2 \cdot p_3 \cdot \cdots \cdot p_n \) and let \( Q = P + 1 \).

Case 1: \( Q \) is prime: Then \( Q \) is a prime different from all of \( p_1, p_2, ..., p_n \) since it is bigger than all of them.

Case 2: \( Q > 1 \) is not prime: Then \( Q \) has some prime factor \( p \) (which must be in the list). Therefore \( p|P \) and \( p|Q \) so \( p|(Q - P) \) which means that \( p|1 \).

Both cases are contradictions so the assumption is false.

\( \blacksquare \)
Famous Algorithmic Problems

• Primality Testing
  – Given an integer $n$, determine if $n$ is prime
• Factoring
  – Given an integer $n$, determine the prime factorization of $n$
Factoring

Factor the following 232 digit number [RSA768]:

123018668453011775513049495838496272077
285356959533479219732245215172640050726
365751874520219978646938995647494277406
384592519255732630345373154826850791702
612214291346167042921431160222124047927
4737794080665351419597459856902143413
Greatest Common Divisor

GCD(a, b):

Largest integer $d$ such that $d \mid a$ and $d \mid b$

- GCD(100, 125) =
- GCD(17, 49) =
- GCD(11, 66) =
- GCD(13, 0) =
- GCD(180, 252) =
GCD and Factoring

\[ a = 2^3 \cdot 3 \cdot 5^2 \cdot 7 \cdot 11 = 46,200 \]
\[ b = 2 \cdot 3^2 \cdot 5^3 \cdot 7 \cdot 13 = 204,750 \]

\[ \text{GCD}(a, b) = 2^{\text{min}(3,1)} \cdot 3^{\text{min}(1,2)} \cdot 5^{\text{min}(2,3)} \cdot 7^{\text{min}(1,1)} \cdot 11^{\text{min}(1,0)} \cdot 13^{\text{min}(0,1)} \]

Factoring is expensive!

Can we compute \( \text{GCD}(a,b) \) without factoring?
Useful GCD Fact

If $a$ and $b$ are positive integers, then
$$\text{gcd}(a, b) = \text{gcd}(b, a \mod b)$$
Useful GCD Fact

If \( a \) and \( b \) are positive integers, then

\[
\gcd(a, b) = \gcd(b, a \mod b)
\]

Proof:

By definition of mod, \( a = qb + (a \mod b) \) for some integer \( q = a \div b \).

Let \( d = \gcd(a, b) \). Then \( d \mid a \) and \( d \mid b \) so \( a = kd \) and \( b = jd \)
for some integers \( k \) and \( j \).

Therefore \( (a \mod b) = a - qb = kd - qjd = (k - qj)d \).
So, \( d \mid (a \mod b) \) and since \( d \mid b \) we must have \( d \leq \gcd(b, a \mod b) \).

Now, let \( e = \gcd(b, a \mod b) \). Then \( e \mid b \) and \( e \mid (a \mod b) \) so
\[
b = me \quad \text{and} \quad (a \mod b) = ne \quad \text{for some integers} \quad m \quad \text{and} \quad n.
\]

Therefore \( a = qb + (a \mod b) = qme + ne = (qm + n)e \).
So, \( e \mid a \) and since \( e \mid b \) we must have \( e \leq \gcd(a, b) \).

It follows that \( \gcd(a, b) = \gcd(b, a \mod b) \).
Another simple GCD fact

If $a$ is a positive integer, $\gcd(a, 0) = a$. 