Lecture 8. Outline.

1. Modular Arithmetic.
   Clock Math!!!
2. Inverses for Modular Arithmetic: Greatest Common Divisor.
3. Euclid’s GCD Algorithm
Clock Math

If it is 1:00 now.

What time is it in 5 hours? 6:00!
What time is it in 15 hours? 16:00!
Actually 4:00.

16 is the “same as 4” with respect to a 12 hour clock system.
Clock time equivalent up to addition/subtraction of 12.

What time is it in 100 hours? 101:00! or 5:00.
5 is the same as 101 for a 12 hour clock system.
Clock time equivalent up to addition of any integer multiple of 12.

Custom is only to use the representative in \{1, \ldots, 11, 12\}
Today is Wednesday.

What day is it a year from now? on September 14, 2017?
Number days.
0 for Sunday, 1 for Monday, \ldots, 6 for Saturday.

Today: day 3.
3 days from now, day 6 or Saturday.
23 days from now, day 26 or day 5, which is Friday!
two days are equivalent up to addition/subtraction of multiple of 7.
9 days from now is day 5 again, Friday!

What day is it a year from now?
Next year is not a leap year. So 365 days from now.
Day 3+365 or day 368.
Smallest representation:
subtract 7 until smaller than 7.
divide and get remainder.
368/7 leaves quotient of 52 and remainder 4.
or September 14, 2017 is Day 4, a Thursday.
Years and years...

80 years from now? September 14, 2096
   20 leap years. 366*20 days
   60 regular years. 365*60 days
It is day $3 + 366 \times 20 + 365 \times 60$. Equivalent to?

Hmm.
   What is remainder of 366 when dividing by 7? 2.
   What is remainder of 365 when dividing by 7? 1
Today is day 3.
   Get Day: $3 + 20 \times 2 + 60 \times 1 = 103$
   Remainder when dividing by 7? 5.
   Or September 14, 2096 is Friday!

Further Simplify Calculation:
   20 has remainder 6 when divided by 7.
   60 has remainder 4 when divided by 7.
Get Day: $3 + 6 \times 2 + 4 \times 1 = 19$.
   Or Day 5.  September 14, 2096 is Friday.

“Reduce” at any time in calculation!
Modular Arithmetic: Basics.

\( x \) is congruent to \( y \) modulo \( m \) or \( "x \equiv y \pmod{m}" \)
if and only if \( (x - y) \) is divisible by \( m \).
...or \( x \) and \( y \) have the same remainder w.r.t. \( m \).
...or \( x = y + km \) for some integer \( k \).

Mod 7 equivalence classes:
\{\ldots, -7, 0, 7, 14, \ldots\} \quad \{\ldots, -6, 1, 8, 15, \ldots\} \ldots

**Useful Fact:** Addition, subtraction, multiplication can be done with any equivalent \( x \) and \( y \).

or \( " a \equiv c \pmod{m} \) and \( b \equiv d \pmod{m} \)
\( \implies a + b \equiv c + d \pmod{m} \) and \( a \cdot b \equiv c \cdot d \pmod{m} \)"

**Proof:** If \( a \equiv c \pmod{m} \), then \( a = c + km \) for some integer \( k \).
If \( b \equiv d \pmod{m} \), then \( b = d + jm \) for some integer \( j \).
Therefore, \( a + b = c + d + (k + j)m \) and since \( k + j \) is integer.
\( \implies a + b \equiv c + d \pmod{m}. \)

Can calculate with representative in \( \{0, \ldots, m - 1\} \).
Notation

$x \pmod{m}$ or $\text{mod } (x, m)$ - remainder of $x$ divided by $m$ in \{0, \ldots, m−1\}.

\[
\text{mod } (x, m) = x - \left\lfloor \frac{x}{m} \right\rfloor m
\]

$\left\lfloor \frac{x}{m} \right\rfloor$ is quotient.

\[
\text{mod } (29, 12) = 29 - \left(\left\lfloor \frac{29}{12} \right\rfloor \right) \times 12 = 29 - (2) \times 12 = 5
\]

Recap:

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

Says two integers $a$ and $b$ are equivalent modulo $m$.

**Modulus** is $m$
Inverses and Factors.

Division: multiply by multiplicative inverse.

\[ 2x = 3 \implies (1/2) \cdot 2x = (1/2)3 \implies x = 3/2. \]

**Multiplicative inverse of** \( x \) is \( y \) where \( xy = 1 \); 
**1 is multiplicative identity element.**

In modular arithmetic, 1 is the multiplicative identity element.

**Multiplicative inverse of** \( x \mod m \) is \( y \) with \( xy = 1 \mod m \).

For 4 modulo 7 inverse is 2: \( 2 \cdot 4 \equiv 8 \equiv 1 \mod 7 \).

Can solve \( 4x = 5 \mod 7 \).

\[ \begin{align*}
2 \cdot 4 & \equiv 2 \cdot 5 \mod 7. \\
8x & \equiv 10 \mod 7. \\
x & \equiv 3 \mod 7.
\end{align*} \]

For 8 modulo 12: no multiplicative inverse!

“Common factor of 4” \( \implies 8k - 12\ell \) is a multiple of four for any \( \ell \) and \( k \) \( \implies 8k \equiv 1 \mod 12 \) for any \( k \).
Greatest Common Divisor and Inverses.

Thm:
If greatest common divisor of \( x \) and \( m \), \( \gcd(x, m) \), is 1, then \( x \) has a multiplicative inverse modulo \( m \).

Proof \( \implies \): The set \( S = \{0x, 1x, \ldots, (m - 1)x\} \) contains \( y \equiv 1 \mod m \) if all distinct modulo \( m \).

Pigeonhole principle: Each of \( m \) numbers in \( S \) correspond to different one of \( m \) equivalence classes modulo \( m \).

\( \implies \) One must correspond to 1 modulo \( m \).

If not distinct, then \( a, b \in \{0, \ldots, m - 1\} \), where
\[
(ax \equiv bx \pmod{m}) \implies (a - b)x \equiv 0 \pmod{m}
\]
Or \( (a - b)x = km \) for some integer \( k \).

\( \gcd(x, m) = 1 \)
\( \implies \) Prime factorization of \( m \) and \( x \) do not contain common primes.
\( \implies (a - b) \) factorization contains all primes in \( m \)'s factorization.
So \( (a - b) \) has to be multiple of \( m \).
\( \implies (a - b) \geq m \). But \( a, b \in \{0, \ldots, m - 1\} \). Contradiction.
**Thm:** If \( \gcd(x, m) = 1 \), then \( x \) has a multiplicative inverse modulo \( m \).

**Proof Sketch:** The set \( S = \{0x, 1x, \ldots, (m - 1)x\} \) contains \( y \equiv 1 \mod m \) if all distinct modulo \( m \).

For \( x = 4 \) and \( m = 6 \). All products of 4...
\[
S = \{0(4), 1(4), 2(4), 3(4), 4(4), 5(4)\} = \{0, 4, 8, 12, 16, 20\}
\]
Reducing \( \mod 6 \)
\[
S = \{0, 4, 2, 0, 4, 2\}
\]
Not distinct. Common factor 2.

For \( x = 5 \) and \( m = 6 \).
\[
S = \{0(5), 1(5), 2(5), 3(5), 4(5), 5(5)\} = \{0, 5, 4, 3, 2, 1\}
\]
All distinct, contains 1! 5 is multiplicative inverse of 5 \( \mod 6 \).

\[
5x = 3 \mod 6 \]
What is \( x \)? Multiply both sides by 5.
\[
x = 15 = 3 \mod 6
\]

\[
4x = 3 \mod 6 \]
No solutions. Can’t get an odd.
\[
4x = 2 \mod 6 \]
Two solutions! \( x = 2, 5 \mod 6 \)

Very different for elements with inverses.
Finding inverses.

How to find the inverse?

How to find if \( x \) has an inverse modulo \( m \)?

Find \( \gcd (x, m) \).

- Greater than 1? No multiplicative inverse.
- Equal to 1? Multiplicative inverse.

Algorithm: Try all numbers up to \( x \) to see if it divides both \( x \) and \( m \).

Very slow.

Next: A Faster algorithm.
Midterm1!!!

Watch Piazza for Logistics!
Watch Piazza for Advice!

Study/review sessions this weekend! See Piazza.

Important reminders:
1. Midterm room assignment: based on your official section enrollment.
2. Grading option form is due tonight. Details are on Piazza.

Any other issues.... Email logistics@eecs70.org / Private message on piazza.

Happy Studying!!!!!!!!!!!!!!!