Mod and Div Functions

The Division Algorithm
For any integer \( n \) and any integer \( d > 1 \),
there are unique integers \( q \) (quotient) and \( r \) (remainder) such that:

\[
\frac{n}{d} = q + \frac{r}{d}, \quad \text{and} \quad r \in \{0, 1, \ldots, d-1\}
\]

Defines two operations:

\[
\begin{align*}
n \mod d &= r \quad \text{and} \quad n \div d = q \\
53 \mod 7 &= 4 \\
53 \div 7 &= 7 \\
53 \mod 1 &= 4 \\
32 \mod 8 &= 0 \\
32 \div 8 &= 4 \\
153 \div 10 &= 15 \\
153 \mod 10 &= 3
\end{align*}
\]

\[
\begin{align*}
-56 \rightarrow -46 \rightarrow -34 \rightarrow -22 \rightarrow -12 \rightarrow -1 \rightarrow 10 \\
\rightarrow -56 \mod 11 &= 10 \\
-56 \div 11 &= -6 \\
-17 \mod 2 &= 1 \\
-17 \div 2 &= -9 \\
-56 \mod 8 &= 0 \\
-56 \div 8 &= -7
\end{align*}
\]

\[
\begin{align*}
n &= d \cdot q + r \\
-56 &= 11 \cdot (-6) + 10
\end{align*}
\]
Modular Arithmetic:

\[
\frac{(332)^7 + 14 \cdot 72}{7} \mod 11
\]

\[
\left[ (332 \mod 11)^7 + (14 \mod 11) \cdot (72 \mod 11) \right] \mod 11.
\]

\[
\left[ 2^7 + 3 \cdot 6 \right] \mod 11 = \left[ 128 \mod 11 + 18 \mod 11 \right] \mod 11
\]

\[
= \left[ 7 + 7 \right] \mod 11 = 3.
\]

\[\Rightarrow \text{In computing arithmetic expressions } \mod n, \text{ can take intermediate results } \mod n.\]

\[
(770 \cdot 372) \mod 7
\]

\[
= (770 \mod 7) \cdot (372 \mod 7)
\]

\[
= 0 \cdot 2 = 0
\]

\[
(5681 \cdot 9^{18} + 7) \mod 2.
\]

\[
(1 \cdot 1 + 1) \mod 2 = 2 \mod 2 = 0.
\]
Equivalence mod $n$

$$x \mod n = y \mod n \iff n \mid (x-y)$$

in which case "$x$ is equivalent to $y$ mod $n$".

$$x \equiv y \mod n.$$

Equivalence mod 4.

\[ (5 \mod -7) = 12 \mod 4. \]

Equivalence classes mod 4: $-13, 2, 67, 53, -101, 42, 7$

\[
\begin{array}{cccccc}
0 & 1 & 2 & 3 \\
53 & 2 & -13 & 67 \\
42 & -101 & 7
\end{array}
\]
The ring $\mathbb{Z}_n$. Ring is a closed mathematical system with addition and multiplication operations.

Obey certain laws (e.g. distributive, associative, etc.)

Identity elements:

- $x + 0 = x$
- $x \cdot 1 = x$

Include polynomials, sequences, matrices, etc.

$\mathbb{Z}_n$: integers mod $n$.

$\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$

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

<table>
<thead>
<tr>
<th>$\times$</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<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>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>2</td>
<td>4</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>3</td>
<td>1</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>4</td>
<td>3</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>
Prime Factorization

Every integer greater than 1 is either prime or composite. Only factors are 1 and itself.

\[ 17, \quad 2, \quad 39 = 3 \cdot 13 \]

Prime, Prime, Composite

Fundamental Theorem of Arithmetic

Every positive integer other than 1 can be expressed uniquely as a product of prime numbers where the primes are written in non-decreasing order.

\[ 48 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 = 2^4 \cdot 3 \]

\[ 84 = 2 \cdot 2 \cdot 3 \cdot 7 \]

Multiplicity of prime \( p \) is the \# of times it appears in the prime factorization.

Multiplicity of 2 in prime factorization of 48 is 4.

Multiplicity of 7 in p.f. of 84 is 1.
Exponential notation in prime factorization:

Each prime appears once — multiplicity in exponent.
Primes in increasing order.

\[ 48 = 2^4 \cdot 3 \]

\[ 84 = 2^2 \cdot 3 \cdot 7 \]

Computing the prime factorization for a # is hard
(we use small examples).

But once you have it, other things become easy

Let \( x + y \) be two integers:

The greatest common divisor \( \gcd(x, y) \)
is the largest number that is a factor of \( x + y \).

The least common multiple \( \text{lcm}(x, y) \)
is the smallest number that is an integer
multiple of \( x + y \).

\[ \gcd(48, 36) = 12 \quad \text{lcm}(48, 12) = 48 \]

\[ \gcd(13, 39) = 13 \quad \text{lcm}(14, 8) = 7 \cdot 8 = 56 \]

\[ \text{gcd}(16, 35) = 1 \quad \text{lcm}(15, 7) = 105 \quad \text{(relatively prime)} \]
\[ 532 = 2^2 \cdot 7 \cdot 19 \]
\[ 648 = 2^3 \cdot 3^4 \]
\[ 1088 = 2^5 \cdot 19^2 \]
\[ 15435 = 3^2 \cdot 5 \cdot 7^3 \]

\[ \gcd(532, 15435) \]
\[ 532 = 2^2 \cdot 3^0 \cdot 5^0 \cdot 7^1 \cdot 19^1 \]
\[ 15435 = 2^0 \cdot 3^2 \cdot 5^1 \cdot 7^2 \cdot 19^1 \]

\[ \gcd = 2^0 \cdot 3^0 \cdot 5^0 \cdot 7^1 \cdot 19^0 = 7 \]

\[ \text{lcm} = 2^2 \cdot 3^1 \cdot 5^1 \cdot 7^3 \cdot 19^1 \]

\[ \gcd(x, y) \cdot \text{lcm}(x, y) = x \cdot y \]
Factoring:

Input: integer $N > 1$.

For $X = 2$ to $N - 1$ if $\sqrt[N]{N}$

If $X$ evenly divides $N$ => return $(X, N/X)$

End

En-for

Return ("Prime").

End

If $N$ is composite, then it has a factor that is at most $\sqrt[N]{N}$.

$N \approx 200$ digits.

$\sqrt[N]{N} \approx 100$ digits. $10^{100}$

Loop takes $10^{10}$ seconds.

$10^{40}$ seconds = $\approx 300 \times 10^{80}$ years.
There is an efficient algorithm for primality testing:

**Factoring**

Input: integer \( N > 1 \).
Output: If \( N \) is prime \( \Rightarrow \) “Prime”
If \( N \) is composite \( \Rightarrow \)
  \[ x \text{ and } y \text{ integers.} \]
  \[ x \cdot y = N. \]

**Primality Testing**

Input: integer \( N > 1 \).
Output: If \( N \) is prime \( \Rightarrow \) “Prime”
If \( N \) is composite \( \Rightarrow \)
  “Composite.”

Hand

Easy.

(Handwritten)
Finding Primes:

Are there large primes?

Euclid showed in 300 B.C.:

There are an infinite number of primes.

Try this: Repeat until success:

Pick a random 200 digit number, p.
Test if p is prime
   If yes, return (p).
   If no, continue.

What is the likelihood of success.

To answer this question, we need to know the density of primes among 200 digit numbers.

This doesn’t quite do it, but it’s close:

Prime Number Theorem:

Let \( \pi(x) \) be the number of prime numbers in the range from 2 to \( x \):

\[
\lim_{x \to \infty} \frac{\pi(x)}{x / \ln(x)} = 1.
\]
A randomly chosen number in the range from 2...x is prime with probability \( \frac{1}{\ln(x)} \).

It takes on average \( \ln(x) \) trials to find a prime number in the range from 2...x.

\[
x \text{ is 200 digits: } \quad \ln(x) \approx 200 \cdot \ln(10) \\
\quad \approx 460
\]