Announcement

• Sign up on Piazza!
  Only \( \approx 72 \) students have enrolled
Outline

1. Russian Peasant Multiplication (RPM)
2. Integer Division
3. Congruence
4. LaTeX Example
Why RPM?

- Understand “algorithm”
- Concept $\rightarrow$ algorithm $\rightarrow$ code
- RPM will turn out to be a familiar algorithm
Russian Peasant Multiplication

\[ M \cdot N = ? \]

[M, N positive for now]

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
</tr>
</thead>
<tbody>
<tr>
<td>2 \cdot M=73</td>
<td>N=41</td>
</tr>
<tr>
<td>2 \cdot 146</td>
<td>20</td>
</tr>
<tr>
<td>2 \cdot 292</td>
<td>10</td>
</tr>
<tr>
<td>2 \cdot 584</td>
<td>5</td>
</tr>
<tr>
<td>2 \cdot 1168</td>
<td>2</td>
</tr>
<tr>
<td>2336</td>
<td>1</td>
</tr>
</tbody>
</table>

B is 1

Add live As 2993
Algorithm Behavior Questions

• Does the algorithm terminate?
• Is it correct?
• How long does it take to run?

These are key CS questions
Algorithm Design Question

- Do we need a growing amount of storage?
- Can add up “live A values” as we go along
- Only remember current A, B, sum
- Three values to remember regardless of size of M, N
Rephrase the Algorithm

- Let $A \leftarrow M$, $B \leftarrow N$, $S \leftarrow 0$
- Repeat
  - If $B$ is odd, $S \leftarrow S + A$
  - $A \leftarrow 2A$
  - $B \leftarrow B \text{DIV} 2$
- Return $S$

- $q = n \text{DIV} d$ denotes integer division: $q$ is the greatest integer such that $qd \leq n$

- $n \; // \; d$ in Python

- More on integer division later

- When do we break out of the “repeat”?
Where to Stop

• Let $A \leftarrow M$, $B \leftarrow N$, $S \leftarrow 0$
• Repeat
  • If $B$ is odd, $S \leftarrow S + A$
  • If $B$ is 1, break
  • $A \leftarrow 2 \times A$
  • $B \leftarrow B \div 2$
• Return $S$

If $B$ is even, then it cannot be 1
A Small but Free Saving

• Let \( A \leftarrow M, B \leftarrow N, S \leftarrow 0 \)
• Repeat
  • If \( B \) is odd
    • \( S \leftarrow S + A \)
    • If \( B \) is 1, break
  • \( A \leftarrow 2 \times A \)
  • \( B \leftarrow B \text{ DIV} \ 2 \)
• Return \( S \)

• Saves about half of the inner “if” evaluations
Russian Peasant Multiplication (RPM)

Pseudocode

**Input:** Two positive integers $M, N$

**Output:** The product $S = MN$

---

$A \leftarrow M$, $B \leftarrow N$, $S \leftarrow 0$

while true do

  if $B$ is odd then
    $S \leftarrow S + A$
  end if

  if $B = 1$ then
    break
  end if

  $A \leftarrow 2A$
  $B \leftarrow B \text{ DIV } 2$

end while

return $S$
Algorithm → Code

• See Homework 1 for a Python implementation...
• ... and for a recursive version
Integer Division

- $n \text{ DIV } d = q$ denotes integer division:
  - $n$ is the dividend
  - $d$ is the divisor
  - $q$ is the quotient
- $q$ is the greatest integer such that $qd \leq n$
- Example: $21 \text{ DIV } 4 = 5$
- We cannot make $q = 5$ any bigger, since $6 \cdot 4 = 24 > 21$
- $r = n - qd = 21 - 5 \cdot 4 = 1$ is the remainder
- $n = qd + r$ with $r < d$
- $r = n \text{ MOD } d$
Same Concept, Different Views

\[ n = qd + r \quad \text{with} \quad r < d \]
\[ 21 = 5 \cdot 4 + 1 \quad \text{with} \quad 1 < 4 \]

\[ q = n \begin{array}{c} \text{DIV} \end{array} d \quad \text{and} \quad r = n \begin{array}{c} \text{MOD} \end{array} d \]
\[ 5 = 21 \begin{array}{c} \text{DIV} \end{array} 4 \quad \text{and} \quad 1 = 21 \begin{array}{c} \text{MOD} \end{array} 4 \]

\[ n = (n \begin{array}{c} \text{DIV} \end{array} d) d + n \begin{array}{c} \text{MOD} \end{array} d \]
\[ 21 = (21 \begin{array}{c} \text{DIV} \end{array} 4) 4 + 21 \begin{array}{c} \text{MOD} \end{array} 4 \]

- \( n \begin{array}{c} \text{MOD} \end{array} d \) pronounced “\( n \) modulo \( d \)”
- the remainder of the division of \( n \) by \( d \)
Congruence

• $n \text{ MOD } d$: remainder of the division of $n$ by $d$
• $m$ and $n$ are congruent modulo $d$ when
  \[(m \text{ MOD } d) = (n \text{ MOD } d)\]
• Notation: $m \equiv n \pmod{d}$ [poor alternative: $m \equiv n \pmod{d}$]
• Example: $13 \equiv 8 \pmod{5}$
• Divide 13 and 8 by 5 → same remainder (3)
A Picture for Integer Division

- divisor (or *modulus*) \( d \): width of the interval
- quotient \( n \ \text{DIV} \ d \): which interval is \( n \) in?
- remainder \( n \ \text{MOD} \ d \): where in the interval is \( n \)?
- congruence \( m \equiv d \ n \): \( m \) and \( n \) are in the same place in their intervals [or at the same point on the circle]
Congruence

• Example:
  • Start counting days from, say, Thursday, January 1\textsuperscript{st}, 1970 to map dates to integers
  • [This is the origin of Unix time]
  • Today $\equiv$ February 4
  • In this context, congruence modulo 7 means “day of the week”

• Congruence in Python:

```python
def congruent(m, n, d):
    assert(d > 0)
    return m % d == n % d
```
\LaTeX\ Example

- Source: congruence.tex
- Output: congruence.pdf

[Click on the file names to inspect the files in your web browser]