CS 113
DISCRETE STRUCTURES

Examples of the Euclidean algorithm for finding GCDs

AN IMPORTANT PROPERTY

- **The division algorithm (a property, really)**
- **Given two integers m and n, you can always find q and r (integers) so that**
  - **$m = nq + r$, with $0 \leq r < n$**

THE EUCLIDEAN ALGORITHM

- **This algorithm is nothing more than repeated application of the division algorithm**
- **This gives a process for finding the gcd of two integers**
- **We call the process the Euclidean algorithm**
- **The next slide contains examples**

EXAMPLES

gcd (301, 238): **301 = 238*1 + 63** **238 = 63*3 + 49** **63 = 49*1 + 14** **49 = 14*3 + 7** **14 = 7*2 + 0** **5 steps. gcd: 7.**	**gcd (533,377):** **533 = 377*1 + 156** **377 = 156*2 + 65** **156 = 65*2 + 26** **65 = 26*2 + 13** **26 = 13*2 + 0** **gcd: 13.**
gcd (532,437): 532 = 437*1 + 95 437 = 95*4 + 57 95 = 57*1 + 38 57 = 38*1 + 19 38 = 19*2 + 0 gcd: 19.	gcd (533,328): 533 = 328*1 + 205 328 = 205*1 + 123 205 = 123*1 + 82 123 = 82*1 + 41 82 = 41*2 + 0 gcd: 41.

A CRUCIAL FACT

- To verify that this works, we need a crucial fact
- Choose two non-zero integers m,n
- Suppose m > n
  - If m=n, the statement below is unnecessary
  - Otherwise, if m < n, switch them around
- The Fact: If m and n are related by m = nq + r, then
    - gcd (m,n) = gcd (n,r)
- The fact is not too hard to verify

VERIFYING THAT MATH

- **Verifying the process for the gcd of 532 and 437 using the crucial fact:**
- **gcd(532, 437) = gcd (437, 95) = gcd (95, 57)**
- **= gcd (57, 38) = gcd (38, 19)**
- **= 19 because 19|38. (The remainder is 0.)**

ANOTHER BENEFIT

- **We also can find a and b (integers) so that**
  - **532a + 437b = 19**
  - **or, in general terms, ma + nb = gcd (m, n)**
- **Just follow the chain backwards**

FOLLOWING THE CHAIN BACKWARDS

- **The gcd is 19**
- **So, from the next to the last line, write**
  - **19 = 57 – 38*1**
- **The line before says 95 = 57*1+38. Solve for 38 and substitute**
  - **19 = 57 – (95 – 57*1)*1**
- **Expand and regroup, based on 57, 95 to get**
  - **19 = 57*2 – 95**
- **Continue**
- **The full process is displayed on the next slide**

SUMMARY

- 19 = 57 – 38 *1
- 19 = 57 – (95 – 57*1)*1
- 19 = 57 – 95 + 57
- 19 = 57*2 – 95
- 19 = (437 – 95*4)*2 – 95
- 19 = 437*2 – 95*8 – 95
- 19 = 437*2 – 95*9
- 19 = 437*2 – (532 – 437)*9
- 19 = 437*2 – 532*9 + 437*9
- So, in summary, 19 = (–11)437 + (9)*532

QUESTIONS

- **Any questions?**