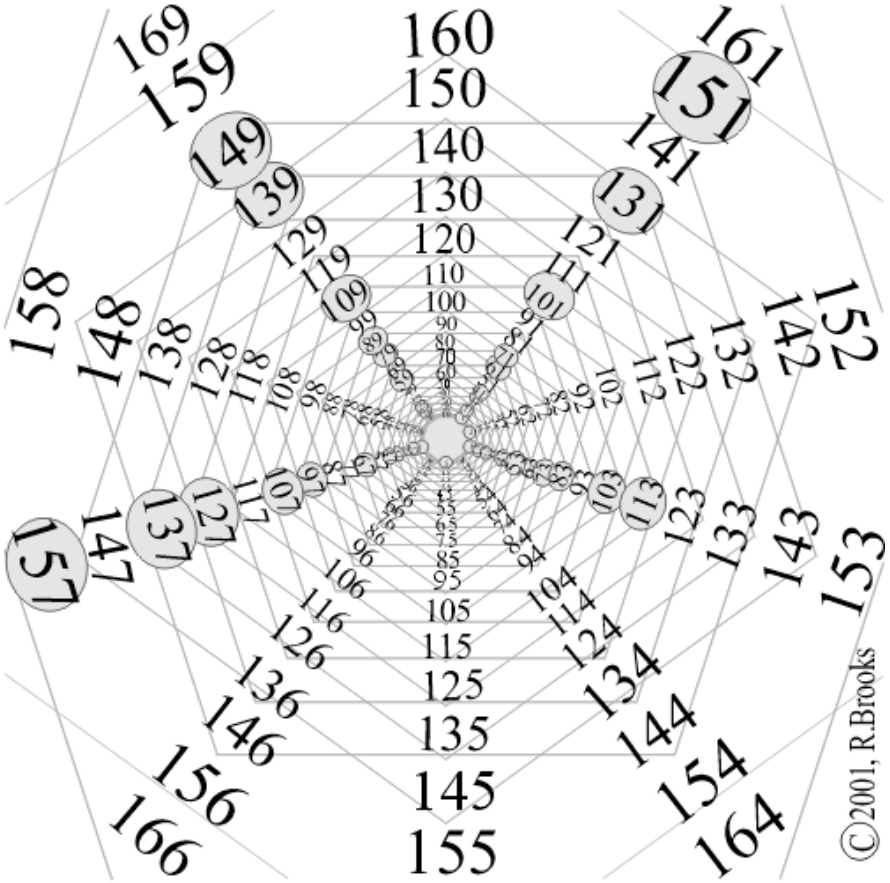
Number Theory: Factors and Primes



http://www.brooksdesign-ps.net/Reginald_Brooks/Code/Html/pin2.htm

Discrete Structures (CS 173)

Gul Agha

Slides based on Derek Hoiem, University of Illinois

Goals of this lecture

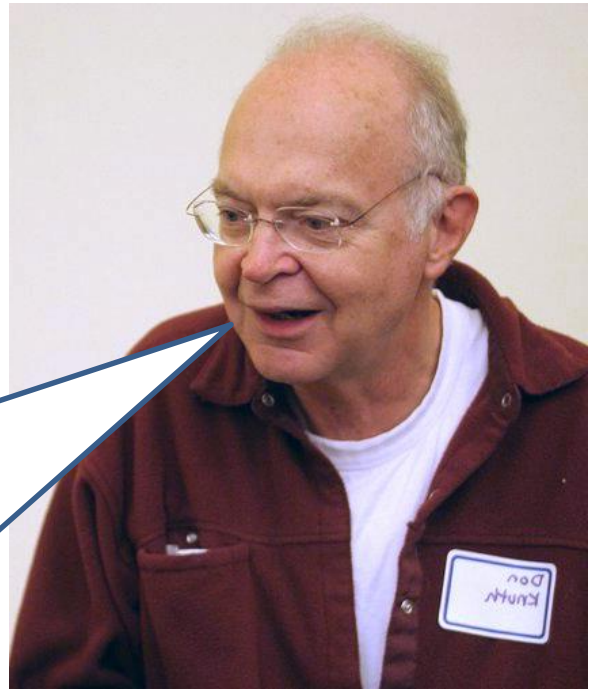
- Understand basic concepts of number theory including divisibility, primes, and factors
- Be able to compute greatest common divisors and least common multiples

Number theory: the study of integers (primes, divisibility, factors, congruence, etc.)

Leonard Dickson
(1874-1954)

Thank God that number theory is unsullied by any application

Virtually every theorem in elementary number theory arises in a natural, motivated way in connection with the problem of making computers do high-speed numerical calculations



Donald Knuth
(quote from 1974)

Other applications include cryptography (e.g., RSA encryption)

http://en.wikipedia.org/wiki/RSA_(algorithm)

Divisibility

Suppose a and b are integers.
Then a divides b iff $b = a\,n$ for some integer n.

Example: $5 \mid 55$ because $55 = 5 * 11$

"a divides b" $\equiv$ "$a \mid b$"

a is a *factor* or *divisor* of b

b is a *multiple* of a

Tip: think "a divides into b"

Examples of divisibility

$$(a \mid b) \leftrightarrow (b = a\,n), \text{ where } n \text{ is some integer}$$

- Which of these holds?

4 | 12

4 | 4

4 | 6

12 | 4

6 | 0

0 | 6

11 | -11

-22 | 11

7 | -15

4 | -16

Proof with divisibility

Claim: For any integers a, b, c, if $a|b$ and b|c, then $a|c$.

Definition: Let a, b be integers, $a|b$ iff $b = a\,n$ for some integer n

Proof with divisibility

Claim: For any integers a, x, y, b, c, if $a|x$ and $a|y$, then $a|(bx + cy)$.

Definition: For all integers a, b, a | b iff $b = a\,n$ for some integer n

overhead

Prime numbers

- Definition: an integer $q \geq 2$ is **prime** if the only positive factors of q are 1 and q.
- Definition: an integer $q \geq 2$ is **composite** if it is not prime.
- Fundamental Theorem of Arithmetic: Every integer ≥ 2 can be written as the product of one or more *prime factors*. This prime factorization is unique:

600=2*2*2*3*5*5

More factor definitions

- *Greatest common divisor* (GCD): $\gcd(a, b)$ is the largest number that divides both a and b
  - Product of shared factors of a and b
- *Least common multiplier* (LCM): $\mathrm{lcm}(a, b)$ is the smallest number that both a and b divide

$$\mathrm{lcm}(a, b) = \frac{ab}{\gcd(a, b)}$$

- Relatively prime: a and b are *relatively prime* if they share no common factors, so that $\gcd(a, b) = 1$

Factor examples

gcd(5, 15) =

gcd(0, k) =

gcd(8, 12) =

gcd(8*m, 12*m) =

gcd(k^3, m*k^2) =

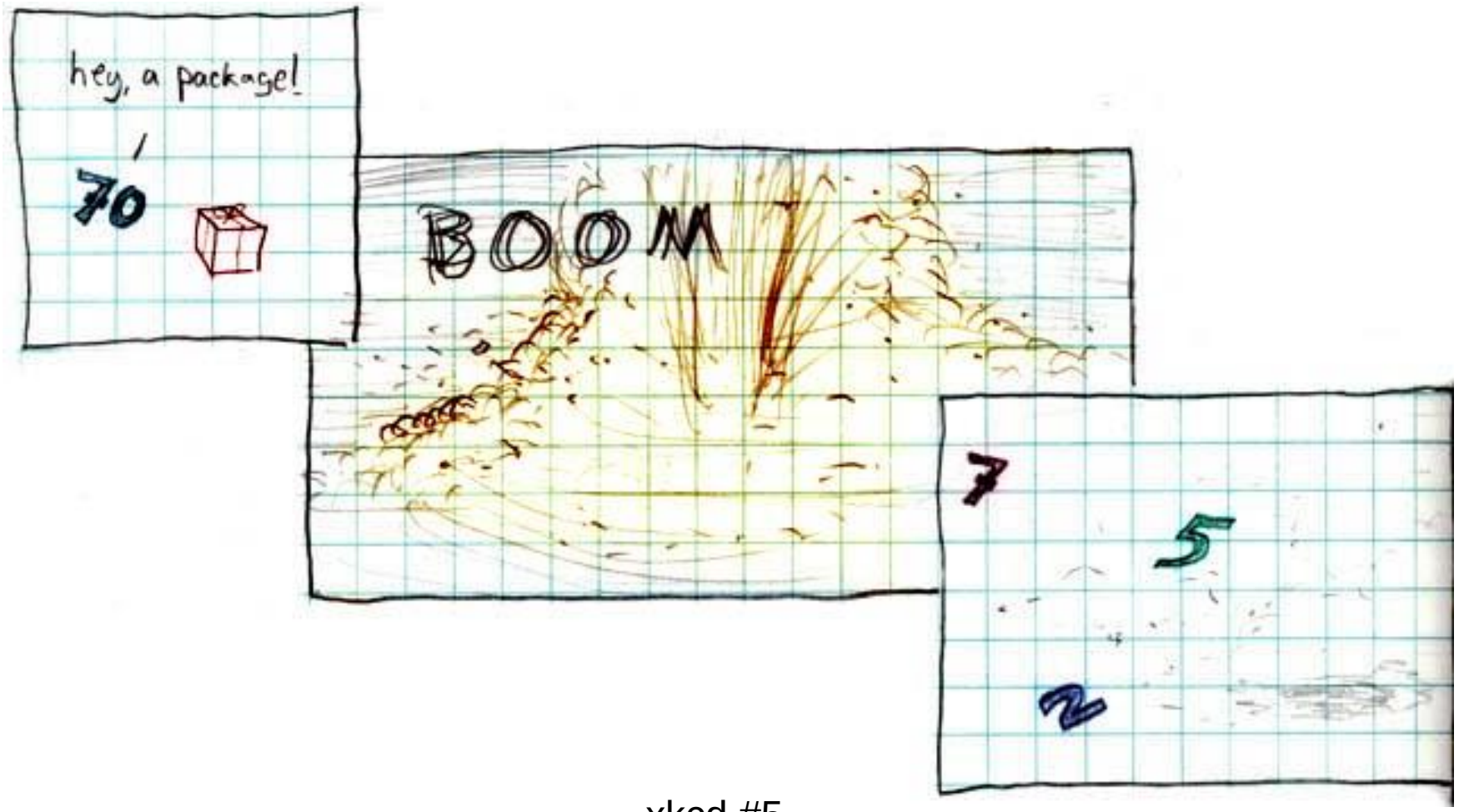
lcm(120, 15) =

lcm (6, 8) =

lcm(0, k) =

Which of these are relatively prime?
6 and 8?
5 and 21?
6 and 33?
3 and 33?
Any two prime numbers?

Short Break



xkcd #5

The Division Algorithm

Theorem 1 (Division Algorithm) *The Division Algorithm: For any integers a and b, where b is positive, there are unique integers q (the quotient) and r (the remainder) such that $a = bq + r$ and $0 \leq r < b$.*

E.g., if $a = 31$ and $b = 5$, $q = 6$ and $r = 1$

Euclid's algorithm for computing gcd

remainder(a, b) is the remainder when a is divided by b

```
gcd(a,b: positive integers)
   x := a
   y := b
   while (y > 0)
      begin
      r := remainder(x,y)
      x := y
      y := r
      end
   return x
```

gcd(969,102)

x	y	r=remainder(x, y)

Euclid's algorithm for computing gcd

remainder(a, b) is the remainder when a is divided by b

```
gcd(a,b: positive integers)
   x := a
   y := b
   while (y > 0)
      begin
      r := remainder(x,y)
      x := y
      y := r
      end
   return x
```

gcd(3289,1111)

x	y	r=remainder(x, y)

Recursive Euclid's Algorithm

```
gcd(a,b: positive integers)
   x := a
   y := b
   while (y > 0)
      begin
      r := remainder(x,y)
      x := y
      y := r
      end
   return x
```

```
procedure gcd(a,b: positive integers)
r := remainder(a,b)
if (r = 0) return b
else return gcd(b,r)
```

But why does Euclid's algorithm work?

```
procedure gcd(a,b: positive integers)
r := remainder(a,b)
if (r = 0) return b
else return gcd(b,r)
```

Euclidean algorithm works because:

1) $\gcd(a,b) = \gcd(b,r)$, where $r = \text{remainder}(a,b)$

2) *r* is always smaller on each call and will eventually be 0

1) says each step of recursion is correct and 2) says the algorithm will terminate

The first part of the proof is gives us *partial correctness,* the first and second give us *total correctness*

Proof of Euclid's algorithm

Claim: For any integers a, b, q, r, with $b > 0$,

if $a = bq + r$ then $\gcd(a, b) = \gcd(b, r)$.

See:

By Proteins - Own work, CC BY-SA 3.0, Geometric illustration of the Proof of Euclid's Algorithm

https://commons.wikimedia.org/w/index.php?curid=6563316

Proof with gcd, relatively prime

Claim: For any integers a, b, c, if a and b are relatively prime, then $\gcd(ab, k) = \gcd(a, k)\gcd(b, k)$.

Definition: Let a, b be integers $a|b$ iff $b = a\,n$ for some integer n

overhead

Next class

- More number theory: congruence and sets