Section 4.3 Number Theory (continued)

Comp 232
Instructor: Robert Mearns

1. Preliminary; Where are we headed in Sections 4.3 ?

Number Theory (study of Integers)

Division

$\frac{a}{d}$ = q + remainder r

(a, d, q, r ∈ Z, d>0, 0≤r<d)

If r = 0 → $\frac{a}{d}$ = q

OR a = d∗q

we say d|a
OR d is
a Factor of a

Congruence

If m | a – b we say:
a ≡ b mod m
a is congruent to b mod m.

Computer Representation

Section 4.2

Prime Integers

- Testing primes
- Finding Prime Factors Fund. Thm. Arithmetic
- Relatively Prime

Least Commom Multiple (lcm)

Greatest Common Divisor (gcd) Euclidean Algorithm

Section 4.3

Another way of looking at Congruence a ≡ b mod m (and b < m):
m | a-b
→ a-b = mq, where q ∈ **Z**
→ a = mq + b

Hence: if a ≡ b mod m (and b < m):

→ b is remainder, when calculating a/m

2. Terms and Definitions

Term	Definition	Example
Prime Integer	If $p \in$ **Z+,** $p>1$ and only factors of p are p and 1 then p is a <u>prime</u> integer Note: 1 is not a prime by definition	$2 = 2 \times 1 \rightarrow 2$ is prime $3 = 3 \times 1 \rightarrow 3$ is prime 4 = 4X1 but 4 = 2X2 → 4 not prime
Composite Integer	If $p \in$ **Z+,** $p>1$ and p is not prime it is called a <u>composite</u> integer	4 is a composite integer
Fundamental Theorem Arithmetic	If $a \in$ **Z+,** $a > 1$ then a can be written as a product of prime integers: $a = p_1 \, p_1 \, p_3 \ldots\ldots\ldots \; p_n$ (p_i are primes)	$100 = 50 \times 2$ $= 25 \times 2 \times 2$ $= 5 \times 5 \times 2 \times 2$
Least Common Multiple	If a, b $\in$ **Z+,** and m is the smallest integer such that $a \mid m$ and $b \mid m$ then m is the <u>Least Common Multiple</u> of a, b. It is denoted lcm(a,b)	lcm (18, 12) = 36. Reason: 36 is the smallest integer such that $18 \mid 36$ and $12 \mid 36$
Greatest Common Divisor	If a, b $\in$ **Z,** not both = 0 and d is the largest integer such that $d \mid a$ and $d \mid b$ then d is the <u>Greatest Common Divisor</u> of a, b. It is denoted gcd(a,b)	Consider a = 24, b = 36 The gcd (24,36) = 12. Reason: 12 is the largest integer that divides both 24 and 36
Relatively Prime integers	If the gcd (a,b) = 1 then a, b are called <u>relatively prime</u>	gcd (9,11) = 1 $\rightarrow$ 9,11 are relatively prime. <u>Note</u> 9 is not a prime itself. Even integers cannot be relatively prime [ex. gcd(6,8) = 2 $\neq$ 1)]

3. An Algorithm (step by step process) to test an integer to see if it is prime.

a) There is a Theorem that will reduce the numbers that we have to test to see if they are prime
Theorem: If n is a composite integer then n has a prime divisor d ≤ $\sqrt{n}$
Proof (by contradiction)

1.	Consider n = a b → a | n and b | n	Given n composite → it has 2 factors ≠1
2.	Either a≤sqrt(n) or b≤sqrt(n) or ¬((a≤sqrt(n) or b≤sqrt(n))	All possible conclusions
3.	Assume ¬(a≤sqrt(n) or b≤sqrt(n))	Assume the one you do not want
4.	→a>sqrt(n) and b>sqrt(n))	DeMorgan, def ¬ (≤)
5.	n = ab > sqrt(n)*sqrt(n) = n	Substitute in line 1 then multiply
6.	→ n > n	Transitive line 5
7.	→ Contradiction	Line 6
8.	Conclusion: a≤sqrt(n) or b≤sqrt(n)	Remaining conclusion possibility

b) We will use the contrapositive form of the Theorem when testing an integer to see if it is prime.

If n does not have a prime divisor d≤sqrt(n) then n is not composite (it is prime)

The Contrapositive form will reduce the numbers we have to test

c) Algorithm: Test a number n to see if it is prime

Step 1: Take the square root of n
Step 2: List all primer ≤ sqrt(n)
Step 3: Test each answer to Step 2 to see if it divides n

Ex: Is 101 prime ?

Step 1 sqrt(101) = 10.04

Step 2 primes $\leq$ 10.04 are 2, 3, 5, 7

Step 3 $2 \nmid 101, \quad 3 \nmid 101, \quad 5 \nmid 101, \quad 7 \nmid 101$

$\rightarrow$ 101 is prime

4. Theorem. There exists is no greatest prime

a) Proof (by contradiction)

Either $\exists$ no greatest prime or $\exists$ a greatest prime

Assume $\exists$ a greatest prime (call it pn)

Let list of all primes be:

where is the greatest

Consider $Q = p_1\ p_2\ p_3\ p_4 \ldots p_n + 1$

$(q_1\ q_2\ q_3\ q_4 \ldots q_m) - (p_1\ p_2\ p_3\ p_4 \ldots p_n) = 1$

$\exists$ At least one of the q_j = one of the p_i

Call the common prime c ($c \neq 1$ since 1 is not prime)

$c\,(q_1\ q_2\ q_3\ q_4 \ldots\ldots\ldots - p_1\ p_2\ p_3\ p_4 \ldots\ldots\ldots\ldots) = 1$

$\rightarrow$ $\exists$ a prime divisor c of the LHS

$\rightarrow$ $\exists$ a prime divisor c of the RHS

$\rightarrow$ $\exists$ a prime divisor c of 1

$\rightarrow$ Contradiction

Conclusion: $\exists$ no greatest prime

List all pos. concl.

Assume poss. not wanted

Mult <u>all</u> primes and add 1

FTA: Q = prod.of primes

Isolate the 1

pi list represents all primes

Factor out common prime

Since LHS = RHS

RHS = 1

Only $1 \mid 1$, and $1 \neq$ prime

b) Use of the Theorem: If you think you have the greatest prime p

5 a) An Algorithm (step by step process) to find the prime factors of an integer n

Step 1 Evaluate $\sqrt{n}$ (Step 1 is optional. It tells you the maximum prime that you might have to test for being a factor

Step 2 Divide n by the smallest prime = 2, then 3, 4, ..., p (p<sqrt(n))

If none of the primes divide n then

n is prime → it has no prime factors
QED

If you get a prime p_i that divides n

get the quotient q
repeat Step 2 with primes < p, using q instead of n

b) This Algorithm shows how to get answer to the <u>Fundamental Theorem of Arithmetic</u> (F.T.A.) which states: All integers greater than one can be expressed as a product of prime integers

Ex: Find the prime factors of 7007

Step 1 $\sqrt{7007} = 83.7 \rightarrow$ We need test only primes ≤ 83.7 to see if they are factors of 7007.

Step 2 (i) primes 2, 3, 5 $\nmid$ 7007

(ii) 7 | 7007 quotient is 1001 → 7007 = 7X1001

(iii) 7 | 1001 quotient is 143 → 7007 = 7X7X143

(iv)

(v) 11 | 143 quotient is 13 → 7007 = 7X7X11X13

(vi)

(vii) 13 | 13 quotient is 1 → 7007 = 7X7X11X13X1

$\rightarrow$ prime factors of 7007 are 7, 11, 13

6. An Algorithm to find the lcm (a,b)

a) This algorithm has been seen many times previously when working with fractions and are asked to find the lowest common denominator.

Ex: Find the lowest common denominator for $\frac{1}{6} + \frac{1}{12} + \frac{1}{9} + \frac{1}{27}$

Step 1 Find prime factors 1/(2*3) + 1/(2*2*3) + 1/(3*3) + 1/(3*3*3)

Step 2 Find lcm of denominators 1/(2*3*2*3*3)

b) Algorithm to find the lcm (a,b)

Step 1 Express each of a, b as a product of primes (find the prime factors for a, b)

Step 2 Form the product of the least number of prime factors needed to factor both a, b

Ex: Find the lcm(18,12)

Step 1 Express both a, b as a product of primes:

18	12
Does 2|18? yes, quotient = 9	Does 2|12? yes, quotient = 6
Does 3|9? yes, quotient = 3	Does 2|6? yes, quotient = 3
Does 3|3? yes, quotient = 1	Does 3|3? yes, quotient = 1
We are done when quotient = 1 Prime factors: 18 = 2X3X3	Prime factors: 12 = 2X2X3

Step 2 The lcm(18,12) = 2X3X3X2 = 36

Do not take all 6 factors. (we want the smallest number that both 18 and 12 divide)

7. Algorithm to find the gcd (a, b)

a) Method 1: Step 1 Find the prime factors of each number a,b

Step 2 Pick out the greatest common factor (divisor) in step 1 answer.

This method is inefficient because it requires finding prime factors which can be a long process if a, b are large numbers. Euclid described a more efficient method.

b) The Euclidean method for determining the gcd(a,d) is based on the following Theorem:

If $a = bq + r$, where $a, b, q, r \in Z$ then $\gcd(a,b) = \gcd(b,r)$

Allows work with smaller numbers b,r:
$b<a$ and $r<b$

Proof:

Step 1 (Direct) Consider $\gcd(a,b) = d$

$d \mid a$ and $d \mid bq \rightarrow d \mid a-bq$ — Def common Divisor

$\rightarrow d \mid r$ — $r = a - bq$

$\rightarrow$ common divisor d of a, b is also common divisor of b, r

Similarly any common divisor of b, r is common divisor of a, b

Step 2 (Contradiction) Either $\gcd(b, r) = d$ — List all possibilities

or $\gcd(b, r) \neq d$

Assume $\gcd(b, r) \neq d$ — Not wanted poss.

Consider gcd(b, r) = , where >d

$\rightarrow$ is a common divisor of a, b and >d — Step 1 last line

$\rightarrow \gcd(a, b) \neq d$ — $d_1 > d$

$\rightarrow$ Contradiction

QED $\gcd(a,b) = \gcd(b,r)$

Method 2: Euclidean method for determining the gcd(a,b)

The previous Theorem justifies the Euclidean method to determine the gcd(a,b)

Step 1 Divide the larger number a by the smaller b to give $a = bq + r_1$

Step 2 Repeat Step 1 with b and r_1 to get $b = r_1 q_1 + r_2$

Step 3 Repeat Step 2 with r_1 and r_2 to get $r_1 = r_2 q_2 + r_3$

Continue the Step 3 process until the remainder $r_i = 0$

Hence $\gcd(a,b) = \gcd(b, r_1) = \gcd(r_1, r_2) = \ldots\ldots\ldots = \gcd(r_{i-2}, r_{i-1}) =$ gcd(ri-1, 0)

Summary: The last non zero remainder

Ex: Find the gcd(287,91)

Step 1 To calculate gcd(287,91): $\frac{287}{91} = 3 +$ rem 14 $\rightarrow$ 287 = 91X3 + remainder 14

Step 2 To calculate gcd (91,14) : $\frac{91}{14} = 6 +$ rem 7 $\rightarrow$ 91 = 14X6 + remainder 7

Step 3 To calculate gcd (14,7) : $\frac{14}{7} = 2 +$ rem 0 $\rightarrow$ 14 = 7X2 + remainder 0

Note: $7 \mid 0 \rightarrow \gcd(7,0) = 7$ (last non zero remainder)

Why ? Listing results above

7 = gcd(7, 0) = gcd(14, 7) = gcd(91, 14) = gcd(287, 91)