

CS103A

10/24/08

Problem Set 7 is due Monday, 11/3. This is one class period later than the date given in the Syllabus.

Outline of topics for CS103A

Basic Tools

- Formal Logic and Proof Techniques
- Number Theory and its Applications
- Proving "Real" Theorems
- Induction
- Program Proofs
- Recursion
- Combinatorics & Probability
- Functions

Number Theory

We will not try to develop number theory from the ground up, but we should acknowledge that this can be done from a small number of axioms.

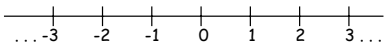
One example: Peano's Axioms, proposed by Giuseppe Peano (1858 - 1932) in 1889.

Peano's Axioms

- There is a number 0.
- Every number has a successor, denoted by $S(a)$.
- There is no number whose successor is 0, i.e., $\forall x (S(x) \neq 0)$.
- Two numbers with the same successor are themselves equal, i.e., $\forall x \forall y (S(x) = S(y) \rightarrow x = y)$
- If a property is possessed by 0 and if the successor of every number possessing the property also possesses it, then it is possessed by every number, i.e., $[Q(0) \wedge \forall x (Q(x) \rightarrow Q(S(x)))] \rightarrow \forall x Q(x)$

What we assume

- The existence of \mathbb{Z} , the set of all integers.

$$\mathbb{Z} = \{\dots -3, -2, -1, 0, 1, 2, 3, \dots\}$$


- Commutativity: $a + b = b + a$
 $a \times b = b \times a$
- Associativity: $(a + b) + c = a + (b + c)$
 $(a \times b) \times c = a \times (b \times c)$
- Distributivity: $a \times (b + c) = a \times b + a \times c$
 $(a + b) \times c = a \times c + b \times c$

What we assume

- $a + 0 = a$
- $a \times 1 = a$
- Negative numbers: the equation $a + x = 0$ has the unique solution $x = -a$.
- Subtraction: $x = b - a \Leftrightarrow a + x = b$
- The integers are closed under addition, multiplication, and subtraction, i.e., if a and b are integers, then so are $a + b$, $a \times b$, and $a - b$.
- The usual algebraic manipulations such as factoring polynomials, raising to powers, etc.

Division

Definition: If a and b are integers and $a \neq 0$, then the statement that a divides b means that there is an integer c such that $b = ac$.

Our notation for " a divides b " is $a \mid b$.

Our notation for " a does not divide b " is $a \nmid b$.

Note that:

Every integer divides 0 (since $0 = a \cdot 0$ for all a).
1 divides every integer.
Every integer divides itself.

Prove: For all integers a , b , and d , if $d \mid a$ and $d \mid b$ then $d \mid (a \pm b)$.

PROOF: By the definition of divides, there are integers s and t such that

$$\begin{aligned} ds &= a \\ \text{and} \quad dt &= b \end{aligned}$$

Adding the two equations and factoring gives

$$d(s + t) = a + b$$

Since $s + t$ is an integer, $d \mid (a + b)$ by the definition of divides. Similarly, $d \mid (a - b)$.
Q.E.D.

Q.E.D.

Quod erat demonstrandum

That which was to be demonstrated

Which was to be proven

■

□

Prove: For all integers a , b , and c , if $a \mid b$ then $a \mid bc$.

Example: $3 \mid 15$, so 3 divides any multiple of 15: 30, 45, ...

Prove: For all integers a , b , and c , if $a \mid b$ then $a \mid bc$.

Example: $3 \mid 15$, so 3 divides any multiple of 15: 30, 45, ...

PROOF: If $a \mid b$, then there exists an integer d such that

$$ad = b$$

If c is any integer, multiplying both sides by c gives

$$\begin{aligned} \text{or} \quad adc &= bc \\ a(dc) &= bc \end{aligned}$$

Since dc is an integer, $a \mid bc$

by the definition of divides. QED.

Prove: For all integers a , b , and c , if $a \mid b$ and $b \mid c$ then $a \mid c$.

Example: $2 \mid 6$ and $6 \mid 42$, so $2 \mid 42$.

Prove: For all integers a , b , and c , if $a \mid b$ and $b \mid c$ then $a \mid c$.

Example: $2 \mid 6$ and $6 \mid 42$, so $2 \mid 42$.

PROOF:

Statement	Reason
There are integers m, n such that $am = b$ and $bn = c$	Def. of divides
$amn = c$	Subs. am for b
$a(mn) = c$	Associativity
mn is an integer	Int closed under mult
$a \mid c$	Def. of divides

The Division Theorem
 Let a be an integer and let d be a positive integer. Then there exist unique integers q and r , with $0 \leq r < d$ such that $a = dq + r$.

r is called the **remainder of a divided by d** and q is called the **quotient**.

Definition: Suppose a and b are integers, not both zero. The largest integer d such that $d \mid a$ and $d \mid b$ is called the **greatest common divisor** of a and b . We denote this as $d = \gcd(a, b)$. If $\gcd(a, b) = 1$, then a and b are said to be **relatively prime**.

	Divisors						
12	1	2	3	4	6	12	$\gcd = 6$
18	1	2	3	6	9	18	
4	1	2	4				$\gcd = 1$
15	1	3	5	15			

Some properties of gcd

$\gcd(a, b) = \gcd(b, a)$
 $\gcd(a, b) = \gcd(-a, b)$
 $\gcd(a, b) = \gcd(|a|, |b|)$
 $\gcd(a, 0) = |a|$
 $\gcd(a, ka) = |a|$ where k is an integer

Examples

$\gcd(756, 210) = \gcd(210, 756) = 42$
 $\gcd(-756, 210) = 42$
 $\gcd(-756, -210) = 42$
 $\gcd(-210, 0) = 210$
 $\gcd(-210, 420) = 210$

Some properties of gcd

If $a = bq + r$ for integers a, b, q , and r , then $\gcd(a, b) = \gcd(b, r)$.

Some properties of gcd

If $a = bq + r$ for integers a, b, q , and r , then $\gcd(a, b) = \gcd(b, r)$.

Suppose we want to find $\gcd(66, 45)$

Since $66 = 45 \cdot 1 + 21$, we can solve the "simpler" problem of finding $\gcd(45, 21)$.

Euclid's Algorithm

```

gcd(a, b)
{
  if a = 0 return |b|
  if b = 0 return |a|
  repeat
  {
    r := a mod b
    a := b
    b := r
  }
  until r = 0
  return a
}
    
```

← The remainder of a divided by b

Euclid's Algorithm

a	b	r
<hr style="width: 100%;"/>	<hr style="width: 100%;"/>	<hr style="width: 100%;"/>
66	45	

```

gcd(a, b)
{
  if a = 0 return |b|
  if b = 0 return |a|
  repeat
  {
    r := a mod b
    a := b
    b := r
  }
  until r = 0
  return a
}
    
```

Euclid's Algorithm

a	b	r
<hr style="width: 100%;"/>	<hr style="width: 100%;"/>	<hr style="width: 100%;"/>
66	45	21

```

gcd(a, b)
{
  if a = 0 return |b|
  if b = 0 return |a|
  repeat
  {
    r := a mod b
    a := b
    b := r
  }
  until r = 0
  return a
}
    
```

Euclid's Algorithm

a	b	r
<hr style="width: 100%;"/>	<hr style="width: 100%;"/>	<hr style="width: 100%;"/>
66	45	21
45	21	3

```

gcd(a, b)
{
  if a = 0 return |b|
  if b = 0 return |a|
  repeat
  {
    r := a mod b
    a := b
    b := r
  }
  until r = 0
  return a
}
    
```

Euclid's Algorithm

a	b	r
<hr style="width: 100%;"/>	<hr style="width: 100%;"/>	<hr style="width: 100%;"/>
66	45	21
45	21	3

```

gcd(a, b)
{
  if a = 0 return |b|
  if b = 0 return |a|
  repeat
  {
    r := a mod b
    a := b
    b := r
  }
  until r = 0
  return a
}
    
```

Euclid's Algorithm

a	b	r
<hr style="width: 100%;"/>	<hr style="width: 100%;"/>	<hr style="width: 100%;"/>
66	45	21
45	21	3
21	3	3

```

gcd(a, b)
{
  if a = 0 return |b|
  if b = 0 return |a|
  repeat
  {
    r := a mod b
    a := b
    b := r
  }
  until r = 0
  return a
}
    
```

Euclid's Algorithm

	a	b	r
gcd(a, b)	66	45	21
{ if a = 0 return b	45	21	3
if b = 0 return a	21	3	0
repeat			
{			
r := a mod b			
a := b			
b := r			
}			
until r = 0			
return a			
}			

Euclid's Algorithm

	a	b	r
gcd(a, b)	66	45	21
{ if a = 0 return b	45	21	3
if b = 0 return a	21	3	0
repeat			
{			
r := a mod b			
a := b			
b := r			
}			
until r = 0			
return a			
}			

Euclid's Algorithm

	a	b	r
gcd(a, b)	28	15	13
{ if a = 0 return b	15	13	2
if b = 0 return a	13	2	1
repeat			
{			
r := a mod b			
a := b			
b := r			
}			
until r = 0			
return a			
}			

Euclid's Algorithm

	a	b	r
gcd(a, b)	243	1281	243
{ if a = 0 return b	1281	243	
if b = 0 return a			
repeat			
{			
r := a mod b			
a := b			
b := r			
}			
until r = 0			
return a			
}			

Prime Numbers

The statement that an integer $n > 1$ is **prime** means that if $n = rs$ for positive integers r and s , then $r = 1$ or $s = 1$.

That is, the only divisors of n are itself and 1.

2, 3, 5, 7, ..., 17, ..., 73, ..., 467, ..., 823, ..., 983, 991, 997, ...

Prime Numbers

The statement that an integer $n > 1$ is **prime** means that if $n = rs$ for positive integers r and s , then $r = 1$ or $s = 1$.

That is, the only divisors of n are itself and 1.

2, 3, 5, 7, ..., 17, ..., 73, ..., 467, ..., 823, ..., 983, 991, 997, ...

$2^{43,112,609} - 1$

Prime Numbers

The statement that an integer $n > 1$ is **prime** means that if $n = rs$ for positive integers r and s , then $r = 1$ or $s = 1$.

That is, the only divisors of n are itself and 1.

2, 3, 5, 7, ..., 17, ..., 73, ..., 467, ..., 823, ..., 983, 991, 997, ...

243,112,609 - 1 12,978,189 **digits**

Discovered Aug. 23, 2008
 by
 Edson Smith, George Woltman, Scott Kurowski
 UCLA

The statement that an integer $n > 1$ is **prime** means that if $n = rs$ for positive integers r and s , then $r = 1$ or $s = 1$.

That is, the only divisors of n are itself and 1.

The statement that an integer $n > 1$ is **composite** means that n is not prime.

That is, $n = rs$ for some positive integers r and s with $r \neq 1$ and $s \neq 1$.

Some Theorems Involving Prime Numbers

Theorem: **If p is prime and $p \mid ab$, then $p \mid a$ or $p \mid b$.**

Some Theorems Involving Prime Numbers

Theorem: **If p is prime and $p \mid ab$, then $p \mid a$ or $p \mid b$.**

Theorem: **If p is prime and $p \mid a_1 a_2 \dots a_n$, then $p \mid a_i$ for some i .**

The Fundamental Theorem of Arithmetic:

Every positive integer greater than 1 can be written uniquely as the product of primes. (Note: a prime number p is considered to be, by itself, a product with a single term, and we mean unique except for the ordering of the primes in the product.)

$8100 = 2 \cdot 2 \cdot 3 \cdot 3 \cdot 3 \cdot 3 \cdot 5 \cdot 5 = 2^2 \cdot 3^4 \cdot 5^2$

Some Theorems Involving Prime Numbers

Theorem: **If p is prime and $p \mid ab$, then $p \mid a$ or $p \mid b$.**

Theorem: **If p is prime and $p \mid a_1 a_2 \dots a_n$, then $p \mid a_i$ for some i .**

The Fundamental Theorem of Arithmetic:

Every positive integer greater than 1 can be written uniquely as the product of primes. (Note: a prime number p is considered to be, by itself, a product with a single term, and we mean unique except for the ordering of the primes in the product.)

$8100 = 2 \cdot 2 \cdot 3 \cdot 3 \cdot 3 \cdot 3 \cdot 5 \cdot 5 = 2^2 \cdot 3^4 \cdot 5^2$

$n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$