Basic Number Theory

Zeph Grunschlag

Announcement

Last 4 problems will be added tonight to HW4.

Agenda

Section 2.3

- Divisors
- Primality
- Fundamental Theorem of Arithmetic
- Division Algorithm
- Greatest common divisors/least common multiples
- Relative Primality
- Modular arithmetic
- Caesar's Cipher

Importance of Number Theory

- Before the dawn of computers, many viewed number theory as last bastion of "pure math" which could not be useful and must be enjoyed only for its aesthetic beauty.
- No longer the case. Number theory is crucial for encryption algorithms. Of utmost importance to everyone from Bill Gates, to the CIA, to Osama Bin Laden.
- E.G., of great importance in COMS 4180 "Network Security".

Importance of Number Theory

The encryption algorithms depend heavily on modular arithmetic. We need to develop various machinery (notations and techniques) for manipulating numbers before can describe algorithms in a natural fashion.

First we start with divisors.

Divisors

DEF: Let a, b and c be integers such that

$$a = b \cdot c .$$

Then b and c are said to ***divide*** (or are ***factors***) of a, while a is said to be a ***multiple*** of b (as well as of c). The pipe symbol "|" denotes "divides" so the situation is summarized by:

$$b \mid a \wedge c \mid a .$$

NOTE: Students find notation confusing, and think of "|" in the reverse fashion, perhaps confuse pipe with forward slash "/"

Divisors. Examples

Q: Which of the following is true?

1. 77 | 7
2. 7 | 77
3. 24 | 24
4. 0 | 24
5. 24 | 0

Divisors. Examples

A:

1. 77 | 7: false bigger number can't divide smaller positive number
2. 7 | 77: true because $77 = 7 \cdot 11$
3. 24 | 24: true because $24 = 24 \cdot 1$
4. 0 | 24: false, only 0 is divisible by 0
5. 24 | 0: true, 0 is divisible by every number ($0 = 24 \cdot 0$)

Formula for Number of Multiples up to given *n*

Q: How many positive multiples of 15 are less than 100?

Formula for Number of Multiples up to given *n*

A: Just list them:

15, 30, 45, 60, 75, 80, 95.

Therefore the answer is 6.

Q: How many positive multiples of 15 are less than 1,000,000?

Formula for Number of Multiples up to Given *n*

A: Listing is too much of a hassle. Since 1 out of 15 numbers is a multiple of 15, if 1,000,000 were were divisible by 15, answer would be exactly 1,000,000/15. However, since 1,000,000 isn't divisible by 15, need to round down to the highest multiple of 15 less than 1,000,000 so answer is $\lfloor 1{,}000{,}000/15 \rfloor$.

In general: The number of d-multiples less than N is given by:

$$|\{m \in \mathbf{Z}^+ \mid d \mid m \text{ and } m \leq N\}| = \lfloor N/d \rfloor$$

Divisor Theorem

THM: Let *a, b,* and *c* be integers. Then:

1. $a|b \wedge a|c \rightarrow a|(b+c)$
2. $a|b \rightarrow a|bc$
3. $a|b \wedge b|c \rightarrow a|c$

EG:

1. $17|34 \wedge 17|170 \rightarrow 17|204$
2. $17|34 \rightarrow 17|340$
3. $6|12 \wedge 12|144 \rightarrow 6 \mid 144$

Divisor Theorem. Proof of no. 2

In general, such statements are proved by starting from the definitions and manipulating to get the desired results.

EG. *Proof of no. 2* ($a|b \rightarrow a|bc$):

Suppose $a|b$. By definition, there is a number m such that $b = am$. Multiply both sides by c to get $bc = amc = a(mc)$. Consequently, bc has been expressed as a times the integer mc so by definition of "|", $a|bc$ 蛸

Prime Numbers

DEF: A number $n \geq 2$ ***prime*** if it is only divisible by 1 and itself. A number $n \geq 2$ which isn't prime is called ***composite***.

Q: Which of the following are prime?

0,1,2,3,4,5,6,7,8,9,10

Prime Numbers

A: 0, and 1 not prime since not positive and greater or equal to 2

2 is prime as 1 and 2 are only factors

3 is prime as 1 and 3 are only factors.

4,6,8,10 not prime as *non-trivially* divisible by 2.

5, 7 prime.

$9 = 3 \cdot 3$ not prime.

Last example shows that not all odd numbers are prime.

Fundamental Theorem of Arithmetic

- THM: Any number $n \geq 2$ is expressible as as a unique product of 1 or more prime numbers.
- Note: prime numbers are considered to be "products" of 1 prime.
- We'll need induction and some more number theory tools to prove this.
- Q: Express each of the following number as a product of primes: 22, 100, 12, 17

Fundamental Theorem of Arithmetic

A: $22 = 2 \cdot 11$, $100 = 2 \cdot 2 \cdot 5 \cdot 5$,
$12 = 2 \cdot 2 \cdot 3$, $17 = 17$

Convention: Want 1 to also be expressible as a product of primes. To do this we define 1 to be the "empty product". Just as the sum of nothing is by convention 0, the product of nothing is by convention 1.

➔Unique factorization of 1 is the factorization that uses no prime numbers at all.

Primality Testing

Prime numbers are very important in encryption schemes. Essential to be able to verify if a number is prime or not. It turns out that this is quite a difficult problem. First try:

```
boolean isPrime(integer n)
  if ( n < 2 ) return false
  for(i = 2 to n -1)
    if( i | n )        // "divides"! not disjunction
      return false
  return true
```

Q: What is the running time of this algorithm?

Primality Testing

A: Assuming divisibility testing is a basic operation –so $O(1)$ (*this is an invalid assumption*)– then above primality testing algorithm is $O(n)$.

Q: What is the running time in terms of the input size k?

Primality Testing

A: Consider $n = 1{,}000{,}000$. The input size is $k = 7$ because n was described using only 7 digits. In general we have $n = O(10^k)$. Therefore, running time is $O(10^k)$. REALLY HORRIBLE!

Q: Can we improve algorithm?

Primality Testing

A:

- Don't try number bigger than $n/2$
- After trying 2, don't try any other even numbers, because know n is odd by this point.
- In general, try only smaller prime numbers
- In fact, only need to try to divide by prime numbers no larger than $\sqrt{n}$ as we'll see next:

Primality Testing

LEMMA: If n is a composite, then its smallest prime factor is $\leq \sqrt{n}$

Proof (by contradiction). Suppose the smallest prime factor is $> \sqrt{n}$. Then by the fundamental theorem of arithmetic we can decompose $n = pqx$ where p and q are primes $> \sqrt{n}$ and x is some integer. Therefore $n > \sqrt{n} \cdot \sqrt{n} \cdot x = nx$ implying that $n > n$, which is impossible showing that the original supposition was false and the theorem is correct. 蝻

Primality Testing. Example

EG: Test if 139 and 143 are prime.

List all primes up to $\sqrt{n}$ and check if they divide the numbers.

2: Neither is even

3: Sum of digits trick: 1+3+9 = 13, 1+4+3 = 8 so neither divisible by 3

5: Don't end in 0 or 5

7: 140 divisible by 7 so neither div. by 7

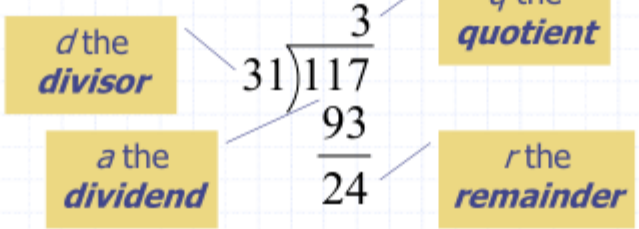
11: Alternating sum trick: 1-3+9 = 7 so 139 not div. By 11. 1-4+3 = 0 so 143 *is* divisible by 11.

STOP! Next prime 13 need not be examined since bigger than $\sqrt{n}$.

Conclude: 139 is prime, 143 is composite.

Division

Remember long division?



$117 = 31 \cdot 3 + 24$

$a = dq + r$

Division

THM: Let a be an integer, and d be a positive integer. There are unique integers q, r with $r \in \{0,1,2,\ldots,d-1\}$ satisfying

$$a = dq + r$$

The proof is a simple application of long-division. The theorem is called the ***division algorithm*** though really, it's long division that's the algorithm, not the theorem.

Greatest Common Divisor Relatively Prime

DEF Let a,b be integers, not both zero. The ***greatest common divisor*** of a and b (or $\gcd(a,b)$) is the biggest number d which divides both a and b.

Equivalently: $\gcd(a,b)$ is smallest number which divisibly by any x dividing both a and b.

DEF: a and b are said to be ***relatively prime*** if $\gcd(a,b) = 1$, so no prime common divisors.

Greatest Common Divisor Relatively Prime

Q: Find the following gcd's:

1. gcd(11,77)
2. gcd(33,77)
3. gcd(24,36)
4. gcd(24,25)

Greatest Common Divisor Relatively Prime

A:

1. gcd(11,77) = 11
2. gcd(33,77) = 11
3. gcd(24,36) = 12
4. gcd(24,25) = 1. Therefore 24 and 25 are relatively prime.

NOTE: A prime number are relatively prime to all other numbers which it doesn't divide.

Greatest Common Divisor Relatively Prime

EG: More realistic. Find gcd(98,420).

Find prime decomposition of each number and find all the common factors:

$98 = 2 \cdot 49 = 2 \cdot 7 \cdot 7$

$420 = 2 \cdot 210 = 2 \cdot 2 \cdot 105 = 2 \cdot 2 \cdot 3 \cdot 35$
$= 2 \cdot 2 \cdot 3 \cdot 5 \cdot 7$

Underline common factors: $\underline{2 \cdot 7} \cdot 7$, $2 \cdot \underline{2} \cdot 3 \cdot 5 \cdot \underline{7}$

Therefore, gcd(98,420) = 14

Greatest Common Divisor Relatively Prime

Pairwise relatively prime: the numbers a, b, c, d, … are said to be pairwise relatively prime if any two distinct numbers in the list are relatively prime.

Q: Find a maximal pairwise relatively prime subset of

{ 44, 28, 21, 15, 169, 17 }

Greatest Common Divisor Relatively Prime

A: A maximal pairwise relatively prime subset of {44, 28, 21, 15, 169, 17} :

{17, 169, 28, 15} is one answer.

{17, 169, 44, 15} is another answer.

Least Common Multiple

DEF: The ***least common multiple*** of *a*, and *b* (lcm(*a*,b)) is the smallest number *m* which is divisible by both *a* and *b*.

Equivalently: lcm(*a*,*b*) is biggest number which divides any *x* divisible by both *a* and *b*

Q: Find the lcm's:

1. lcm(10,100)
2. lcm(7,5)
3. lcm(9,21)

Least Common Multiple

A:

1. lcm(10,100) = 100
2. lcm(7,5) = 35
3. lcm(9,21) = 63

THM: lcm(a,b) = ab / gcd(a,b)

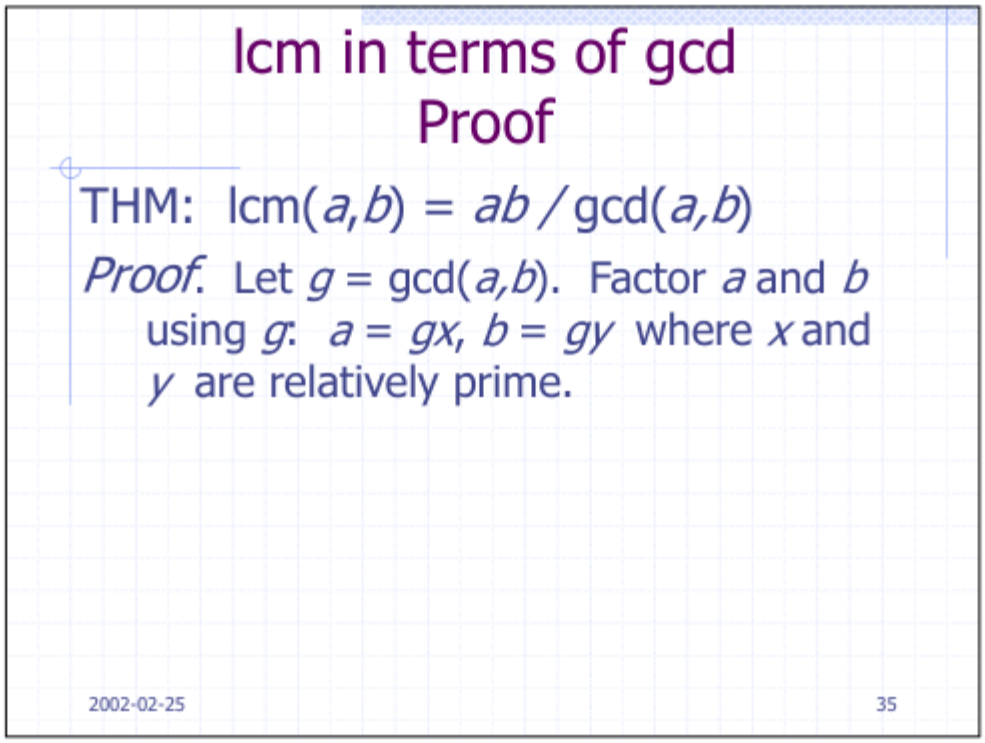
Skip proof in lecture

lcm in terms of gcd Proof

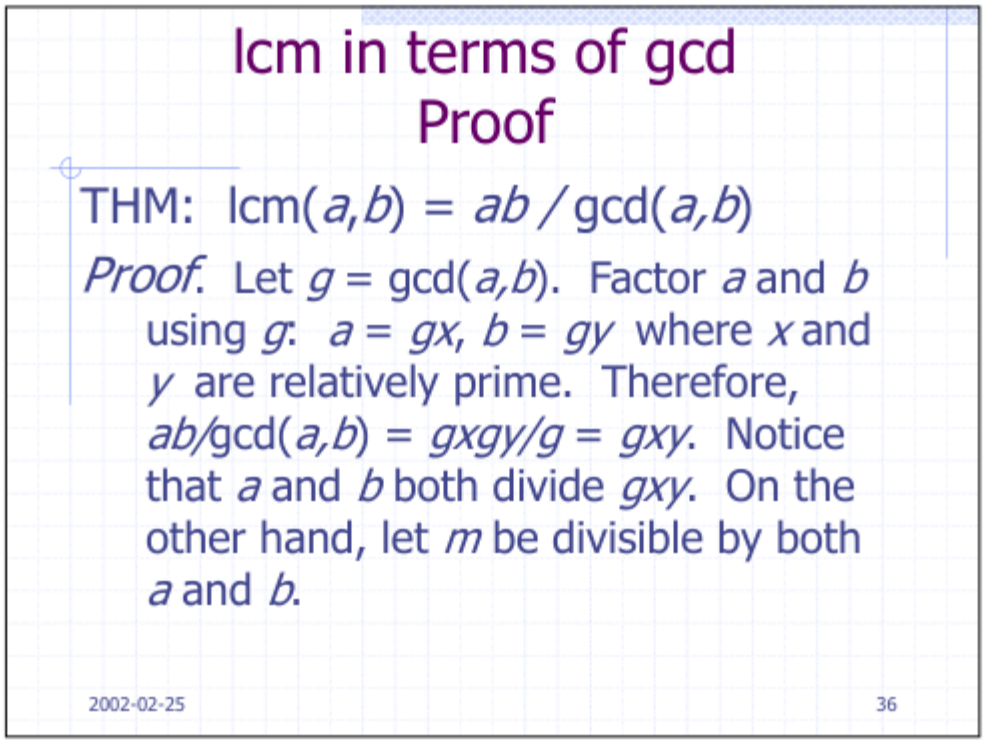
THM: lcm(a,b) = ab / gcd(a,b)

Proof. Let g = gcd(a,b).

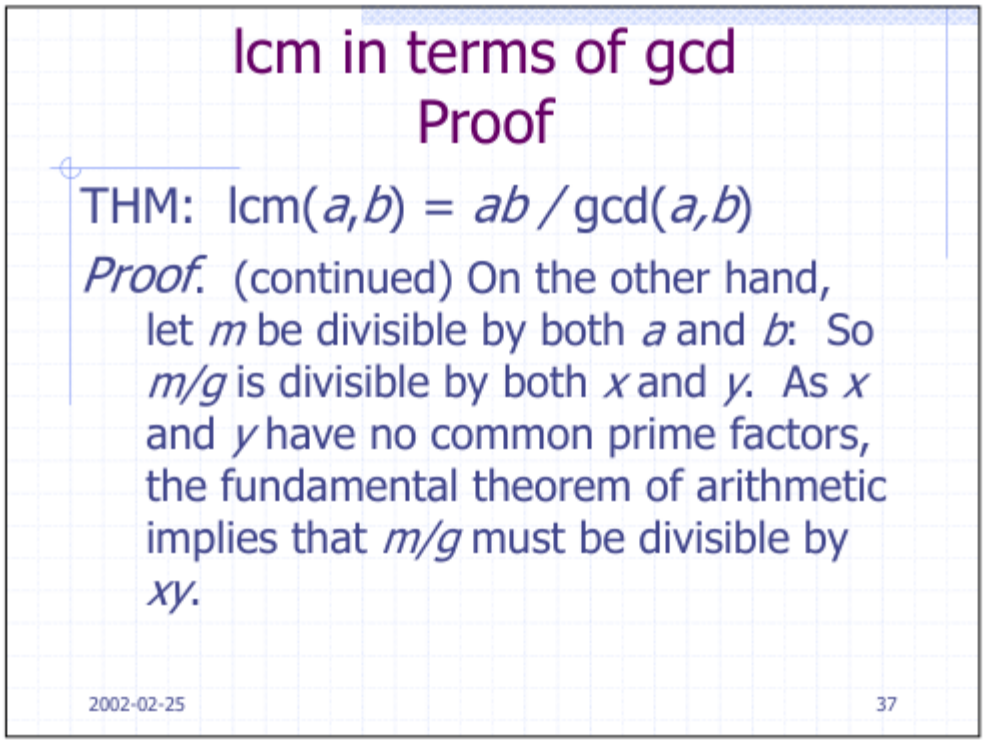
Skip proof in lecture



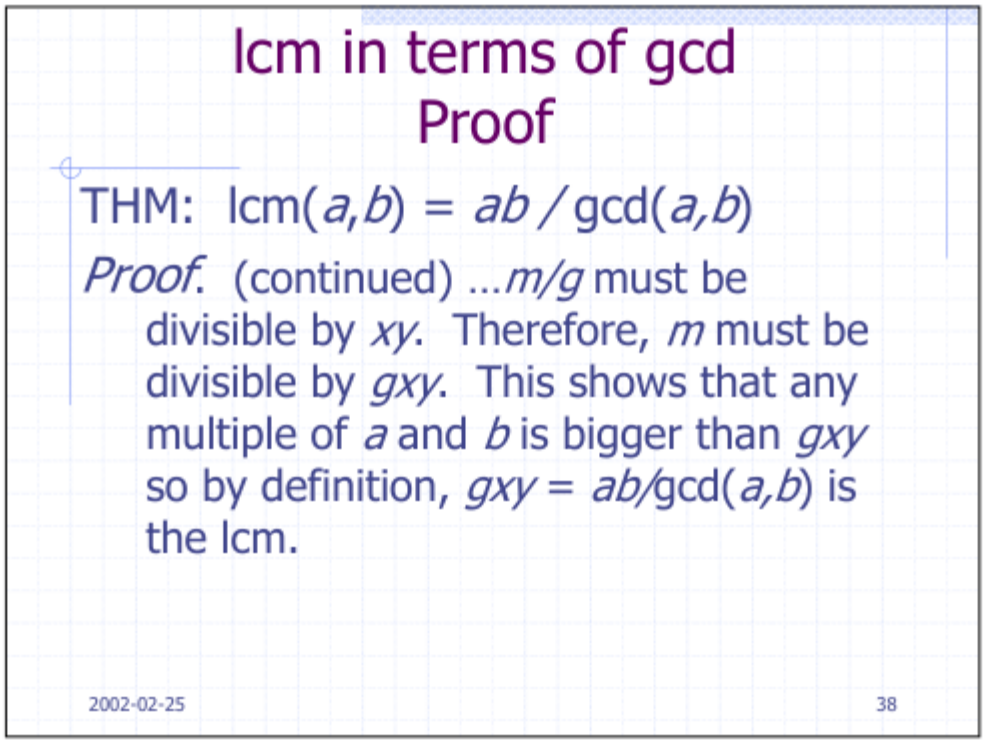
Skip proof in lecture



Skip proof in lecture



Skip proof in lecture



Skip proof in lecture

Modular Arithmetic

There are two types of "mod" (confusing):

- the **mod** function
  - Inputs a number *a* and a base *b*
  - Outputs *a* **mod** *b* a number between 0 and *b* –1 inclusive
  - This is the remainder of a÷b
  - Similar to Java's % operator.
- the (mod) congruence
  - Relates two numbers *a, a'* to each other relative some base *b*
  - $a \equiv a'$ (mod *b*) means that *a* and *a'* have the same remainder when dividing by *b*

mod function

Similar to Java's "%" operator except that answer is always positive. E.G.

-10 **mod** 3 = 2, but in Java –10%3 = -1.

Q: Compute

1. 113 **mod** 24
2. -29 **mod** 7

mod function

A: Compute

1. 113 **mod** 24: $24\overline{)113}$

2. -29 **mod** 7

6

mod function

A: Compute

1. 113 **mod** 24:

$$\begin{array}{r} 4 \\ 24\overline{)113} \\ \underline{96} \\ 17 \end{array}$$

2. -29 **mod** 7

mod function

A: Compute

1. 113 **mod** 24:

$$24\overline{)113}\quad 4,\ 96,\ 17$$

2. -29 **mod** 7

$$7\overline{)-29}$$

mod function

A: Compute

1. 113 **mod** 24:

$$24\overline{)113}\quad 4,\ 96,\ 17$$

2. -29 **mod** 7

$$7\overline{)-29}\quad -5,\ -35,\ 6$$

(mod) congruence Formal Definition

DEF: Let a, a' be integers and b be a positive integer. We say that a is congruent to a' modulo b (denoted by $a \equiv a' \pmod{b}$) iff $b \mid (a - a')$.

Equivalently: $a \bmod b = a' \bmod b$

Q: Which of the following are true?

1. $3 \equiv 3 \pmod{17}$
2. $3 \equiv -3 \pmod{17}$
3. $172 \equiv 177 \pmod{5}$
4. $-13 \equiv 13 \pmod{26}$

(mod) congruence

A:

1. $3 \equiv 3 \pmod{17}$ True. any number is congruent to itself (3-3 = 0, divisible by all)
2. $3 \equiv -3 \pmod{17}$ False. (3-(-3)) = 6 isn't divisible by 17.
3. $172 \equiv 177 \pmod{5}$ True. 172-177 = -5 is a multiple of 5
4. $-13 \equiv 13 \pmod{26}$ True: -13-13 = -26 divisible by 26.

(mod) congruence Identities

The (mod) congruence is useful for manipulating expressions involving the **mod** function. It lets us view modular arithmetic relative a fixed base, as creating a number system inside of which all the calculations can be carried out.

- a **mod** $b \equiv a \pmod{b}$
- Suppose $a \equiv a' \pmod{b}$ and $c \equiv c' \pmod{b}$ Then:
  - $a+c \equiv (a'+c') \pmod{b}$
  - $ac \equiv a'c' \pmod{b}$
  - $a^k \equiv a'^k \pmod{b}$

Modular arithmetic harder examples

Q: Compute the following.

1. 307^{1001} **mod** 102
2. $(-45 \cdot 77)$ **mod** 17
3. $\left(\sum_{i=4}^{23} 10^i\right) \bmod 11$

Modular arithmetic harder examples

A: Use the previous identities to help simplify:

1. Using multiplication rules, before multiplying (or exponentiating) can reduce modulo 102:

307^{1001} **mod** 102 $\equiv 307^{1001} \pmod{102}$

$\equiv 1^{1001} \pmod{102} \equiv 1 \pmod{102}$.

Therefore, 307^{1001} **mod** 102 = 1.

Modular arithmetic harder examples

A: Use the previous identities to help simplify:

2. Repeatedly reduce after each multiplication:

(-45·77) **mod** 17 ≡ (-45·77) (mod 17)

≡(6·9) (mod 17) ≡ 54 (mod 17) ≡ 3 (mod 17). Therefore (-45·77) **mod** 17 = 3.

Modular arithmetic harder examples

A: Use the previous identities to help simplify:

3. Similarly, before taking sum can simplify modulo 11:

$$\left(\sum_{i=4}^{23} 10^i\right) \bmod 11 \equiv \left(\sum_{i=4}^{23} 10^i\right) (\bmod 11) \equiv \left(\sum_{i=4}^{23} (-1)^i\right) (\bmod 11)$$

$$\equiv (1-1+1-1+\ldots+1-1)(\bmod 11) \equiv 0(\bmod 11)$$

Therefore, the answer is 0.

Proving Modular Identities

We first need:

THM: $a \equiv a' \pmod{b} \leftrightarrow \exists k \; a = a' + kb$

Proof. ← direction: If $a = a' + kb$, then $(a-a') = kb$ so that $b \mid (a-a')$ which by definition means that $a \equiv a' \pmod{b}$

→ direction: If $a \equiv a' \pmod{b}$, by definition $b \mid (a-a')$ so for some k we have $(a-a') = kb$ which becomes $a = a' + kb$ 蛹

This is a handy little theorem as we'll see next:

Proving Modular Identities

Prove the identity

$a \equiv a' \pmod{b} \wedge c \equiv c' \pmod{b}$

---→ $ac \equiv a'c' \pmod{b}$

Proof. By the previous, we can assume that there are k and l such that

$a = a' + bk$ and $c = c' + bl$

Thus $ac = (a' + bk)(c' + bl)$

$= a'c' + b(kc' + la' + bkl)$. Therefore

$(ac - a'c') = b(kc' + la' + bkl)$ is divisible by b and hence by definition, $ac \equiv a'c' \pmod{b}$

Simple Encryption

Variations on the following have been used to encrypt messages for thousands of years.

1. Convert a message to capitals.
2. Think of each letter as a number between 1 and 26.
3. Apply an invertible modular function to each number.
4. Convert back to letters (0 becomes 26).

Letter ←→ Number Conversion Table

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

Encryption example

Let the encryption function be

$$f(a) = (3a + 9) \textbf{ mod } 26$$

Encrypt "Stop Thief"

1. STOP THIEF (capitals)
2. 19,20,15,16 20,8,9,5,6
3. 14,17,2,5 17,7,10,24,1
4. NQBE QGJXA

Decryption example

Decryption works the same, except that you apply the inverse function.

EG: Find the inverse of

$$f(a) = (3a + 9) \textbf{ mod } 26$$

If we didn't have to deal with **mod** 26, inverse would be

$$g(a) = 3^{-1}(a - 9)$$

We'll see that since gcd(3,26) = 1, the inverse of 3 is actually well defined modulo 26 and is the number 9. This gives:

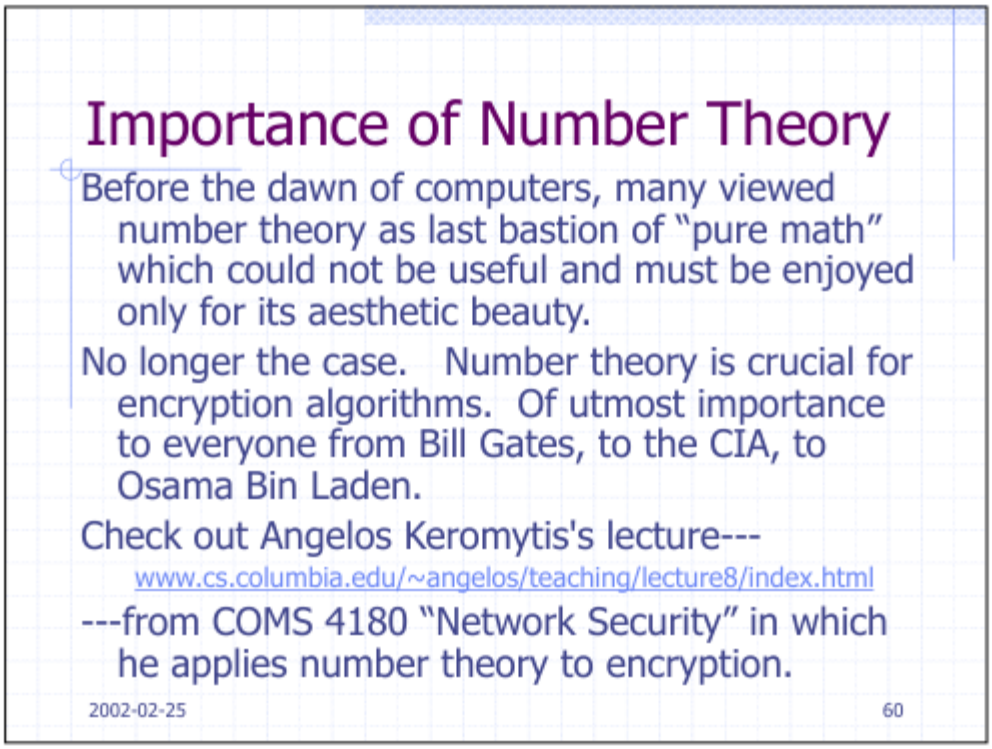
$$g(a) = 9(a - 9) \textbf{ mod } 26 = (9a - 3) \textbf{ mod } 26$$

Caesar's Cipher

$f(a) = (a+3) \bmod 26$

Blackboard Exercise

Prove that there are infinitely many prime numbers. (Discovered by Euclid).



Link not functioning this semester