Number Theory

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. $77 \mid 7$
2. $7 \mid 77$
3. $24 \mid 24$
4. $0 \mid 24$
5. $24 \mid 0$

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 ($0 = 24 \cdot 0$)

Properties of Divisibility

- If $a|1$, then $a = \pm 1$.

- *If $a|b$ and $b|a$, then $a = \pm b$.*
  Any b /= 0 divides 0.

- *If $a \mid b$ and $b \mid c$, then $a \mid c$*
  e.g. 11 | 66 and 66 | 198 x 11 | 198

- If $b|g$ and $b|h$, then $b|(mg + nh)$
  for arbitrary integers m and n
  e.g. $b = 7$; $g = 14$; $h = 63$; $m = 3$; $n = 2$
  hence $7|14$ and $7|63$

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***.

- Integer n can be factored as
  - $n=p_1^{a_1} p_2^{a_2} p_3^{a_3} \ldots p_n^{a_n}$

    where p_i is prime number

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!

Division

Remember long division?

d the ***divisor***

q the ***quotient***

$$\begin{array}{r} 3 \\ 31\overline{)117} \\ \underline{93} \\ 24 \end{array}$$

a the ***dividend***

r the ***remainder***

117 = 31·3 + 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.

Euclidean algorithm

- Find the GCD of two numbers a and b, a<b

- Use fact if a and b have divisor d so does a-b, a-2b …
  - A=a, B=b
  - while B>0
    - R = A mod B
    - A = B, B = R
  - return A

Example GCD(1970,1066)

• 1970 = 1 x 1066 + 904	gcd(1066, 904)
• 1066 = 1 x 904 + 162	gcd(904, 162)
• 904 = 5 x 162 + 94	gcd(162, 94)
• 162 = 1 x 94 + 68	gcd(94, 68)
• 94 = 1 x 68 + 26	gcd(68, 26)
• 68 = 2 x 26 + 16	gcd(26, 16)
• 26 = 1 x 16 + 10	gcd(16, 10)
• 16 = 1 x 10 + 6	gcd(10, 6)
• 10 = 1 x 6 + 4	gcd(6, 4)
• 6 = 1 x 4 + 2	gcd(4, 2)
• 4 = 2 x 2 + 0	gcd(2, 0)

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

mod function

A: Compute

1. 113 **mod** 24:

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

2. -29 **mod** 7

mod function

A: Compute

1. 113 **mod** 24:

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

2. -29 **mod** 7

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

mod function

A: Compute

1. 113 **mod** 24:

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

2. -29 **mod** 7

$$\begin{array}{r} -5 \\ 7\overline{)-29} \\ -35 \\ \hline 6 \end{array}$$

(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: $a \textbf{ mod } b = a' \textbf{ mod } b$

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.

Modular Arithmetic

- **Congruence**
  - a ≡ b mod n says when divided by *n* that a and b have the same remainder
  - It defines a relationship between all integers
    - a ≡ a
    - a ≡ b then b ≡ a
    - a ≡ b, b ≡ c then a ≡ c

Cont.

- **addition**
  - (a+b) mod n ≡(a mod n) + (b mod n)
- **subtraction**
  - a-b mod n ≡ a+(-b) mod n
- **multiplication**
  - a*b mod n
  - derived from repeated addition
  - Possible: a*b ≡ 0 where neither a, b ≡ 0 mod n
    - Example: 2*3 =0 mod 6

Cont.

- **Division**
  - $b/a \bmod n$
  - multiplied by inverse of a: $b/a = b*a^{-1} \bmod n$
  - $a^{-1}*a \equiv 1 \bmod n$
  - $3^{-1} \equiv 7 \bmod 10$ because $3*7 \equiv 1 \bmod 10$
  - Inverse does not always exist!
    - Only when gcd(a,n)=1

Modular Arithmetic

- An Addition Table in Z_{12}

Plus	0	1	2	3	4	5	6	7	8	9	10	11
0	**0**	1	2	3	4	5	6	7	8	9	10	11
1	1	2	3	4	5	6	7	8	9	10	11	**0**
2	2	3	4	5	6	7	8	9	10	11	**0**	1
3	3	4	5	6	7	8	9	10	11	**0**	1	2
4	4	5	6	7	8	9	10	11	**0**	1	2	3
5	5	6	7	8	9	10	11	**0**	1	2	3	4
6	6	7	8	9	10	11	**0**	1	2	3	4	5
7	7	8	9	10	11	**0**	1	2	3	4	5	6
8	8	9	10	11	**0**	1	2	3	4	5	6	7
9	9	10	11	**0**	1	2	3	4	5	6	7	8
10	10	11	**0**	1	2	3	4	5	6	7	8	9
11	11	**0**	1	2	3	4	5	6	7	8	9	10

Additive Inverse Property

- a + -a = 0
- What is the meaning of -a in Z_{12}?
  - If a = 5 then 5 + -5 = 0 translates to
    - 5 + 7 = 0
  - If a = 3 then 3 + -3 = 0 translates to
    - 3 + 9 = 0
- Then -a can be translated as (n – a)

- The Additive Inverse Property
  - The same pattern holds for other n

MOD 4

Plus	0	1	2	3
0	**0**	1	2	3
1	1	2	3	**0**
2	2	3	**0**	1
3	3	**0**	1	2

MOD 5

Plus	0	1	2	3	4
0	**0**	1	2	3	4
1	1	2	3	4	**0**
2	2	3	4	**0**	1
3	3	4	**0**	1	2
4	4	**0**	1	2	3

MOD 9

Plus	0	1	2	3	4	5	6	7	8
0	**0**	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8	**0**
2	2	3	4	5	6	7	8	**0**	1
3	3	4	5	6	7	8	**0**	1	2
4	4	5	6	7	8	**0**	1	2	3
5	5	6	7	8	**0**	1	2	3	4
6	6	7	8	**0**	1	2	3	4	5
7	7	8	**0**	1	2	3	4	5	6
8	8	**0**	1	2	3	4	5	6	7

Multiplicative Inverse Property

- $a * 1/a = 1$
- What is the meaning of $1/a$ in Z_n?
  - $Z_{12} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$
  - There are no fractions
  - Can we find numbers to multiply a given element in Z_{12} such that the product will be one?
  - Definition of division tells us that

    if $1/a = k$ then $k * a = 1$

- A Multiplication Table in Z_{12}

Times	0	1	2	3	4	5	6	7	8	9	10	11
0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	**1**	2	3	4	5	6	7	8	9	10	11
2	0	2	4	6	8	10	0	2	4	6	8	10
3	0	3	6	9	0	3	6	9	0	3	6	9
4	0	4	8	0	4	8	0	4	8	0	4	8
5	0	5	10	3	8	**1**	6	11	4	9	2	7
6	0	6	0	6	0	6	0	6	0	6	0	6
7	0	7	2	9	4	11	6	**1**	8	3	10	5
8	0	8	4	0	8	4	0	8	4	0	8	4
9	0	9	6	3	0	9	6	3	0	9	6	3
10	0	10	8	6	4	2	0	10	8	6	4	2
11	0	11	10	9	8	7	6	5	4	3	2	**1**

Modular Arithmetic

- The Multiplicative Inverse Property: Z_{12}
  - Only 1, 5, 7 and 11 have inverses
    - 5 and 7 are the inverses of each other
    - Both 1 and 11 are their own inverses
    - Why don't the other numbers have inverses?
      - Conjectures?
      - Test with other mods: Try mods 5, 6, 7, 8, 9, 10 and 11
      - But, before you start, look at the table again and look for more patterns.

Modular Arithmetic

- A Multiplication Table in Z_{12}

Times	0	1	2	3	4	5	6	7	8	9	10	11
0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	**1**	2	3	4	5	6	7	8	9	10	11
2	0	2	4	6	8	10	0	2	4	6	8	10
3	0	3	6	9	0	3	6	9	0	3	6	9
4	0	4	8	0	4	8	0	4	8	0	4	8
5	0	5	10	3	8	**1**	6	11	4	9	2	7
6	0	6	0	6	0	6	0	6	0	6	0	6
7	0	7	2	9	4	11	6	**1**	8	3	10	5
8	0	8	4	0	8	4	0	8	4	0	8	4
9	0	9	6	3	0	9	6	3	0	9	6	3
10	0	10	8	6	4	2	0	10	8	6	4	2
11	0	11	10	9	8	7	6	5	4	3	2	**1**

Modular Arithmetic

- The Multiplicative Inverse Property: Z_n
  - For n = 11, 10, 9, 8, 7, 6, 5,…
    - Which numbers have inverses and which do not?
    - Is there a pattern to this?
    - Is there a number in every mod that has a multiplicative inverse (aside from 1)?
    - Let’s look…

- A Multiplication Table in Z_{11}

Times	0	1	2	3	4	5	6	7	8	9	10
0	0	0	0	0	0	0	0	0	0	0	0
1	0	**1**	2	3	4	5	6	7	8	9	10
2	0	2	4	6	8	10	**1**	3	5	7	9
3	0	3	6	9	**1**	4	7	10	2	5	8
4	0	4	8	**1**	5	9	2	6	10	3	7
5	0	5	10	4	9	3	8	2	7	**1**	6
6	0	6	**1**	7	2	8	3	9	4	10	5
7	0	7	3	10	6	2	9	5	**1**	8	4
8	0	8	5	2	10	7	4	**1**	9	6	3
9	0	9	7	5	3	**1**	10	8	6	4	2
10	0	10	9	8	7	6	5	4	3	2	**1**

- A Multiplication Table in Z_{10}

Times	0	1	2	3	4	5	6	7	8	9
0	0	0	0	0	0	0	0	0	0	0
1	0	**1**	2	3	4	5	6	7	8	9
2	0	2	4	6	8	0	2	4	6	8
3	0	3	6	9	2	5	8	**1**	4	7
4	0	4	8	2	6	0	4	8	2	6
5	0	5	0	5	0	5	0	5	0	5
6	0	6	2	8	4	0	6	2	8	4
7	0	7	4	**1**	8	5	2	9	6	3
8	0	8	6	4	2	0	8	6	4	2
9	0	9	8	7	6	5	4	3	2	**1**

- A Multiplication Table in Z_9

Times	0	1	2	3	4	5	6	7	8
0	0	0	0	0	0	0	0	0	0
1	0	**1**	2	3	4	5	6	7	8
2	0	2	4	6	8	**1**	3	5	7
3	0	3	6	0	3	6	0	3	6
4	0	4	8	3	7	2	6	**1**	5
5	0	5	**1**	6	2	7	3	8	4
6	0	6	3	0	6	3	0	6	3
7	0	7	5	3	**1**	8	6	4	2
8	0	8	7	6	5	4	3	2	**1**

- A Multiplication Table in Z_8

Times	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	**1**	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	**1**	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	**1**	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	**1**

- A Multiplication Table in Z_7

Times	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	**1**	2	3	4	5	6
2	0	2	4	6	**1**	3	5
3	0	3	6	2	5	**1**	4
4	0	4	**1**	5	2	6	3
5	0	5	3	**1**	6	4	2
6	0	6	5	4	3	2	**1**

- A Multiplication Table in Z_6

Times	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	**1**	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	**1**

- A Multiplication Table in Z_5

Times	0	1	2	3	4
0	0	0	0	0	0
1	0	**1**	2	3	4
2	0	2	4	**1**	3
3	0	3	**1**	4	2
4	0	4	3	2	**1**

- A Multiplication Table in Z_n: Summary

Z_n	Have Inverse	Don't Have Inverse
12	1, 5, 7, 11	0, 2, 3, 4, 6, 8, 9, 10
11	1, 2, 3, 4, 5, 6, 7, 8, 9, 10	0
10	1, 3, 7, 9	0, 2, 4, 5, 6, 8
9	1, 2, 4, 5, 7, 8	0, 3, 6
8	1, 3, 5, 7	0, 2, 4, 6
7	1, 2, 3, 4, 5, 6	0
6	1, 5	0, 2, 3, 4
5	1, 2, 3, 4	0

- A Multiplication Table in Z_n: Summary

Z_n	Have Inverse	Don't Have Inverse
12	**1**, 5, 7, **11**	**0**, 2, 3, 4, 6, 8, 9, 10
11	**1**, 2, 3, 4, 5, 6, 7, 8, 9, **10**	**0**
10	**1**, 3, 7, **9**	**0**, 2, 4, 5, 6, 8
9	**1**, 2, 4, 5, 7, **8**	**0**, 3, 6
8	**1**, 3, 5, **7**	**0**, 2, 4, 6
7	**1**, 2, 3, 4, 5, **6**	**0**
6	**1**, **5**	**0**, 2, 3, 4
5	**1**, 2, 3, **4**	**0**

Multiplication Table in Z_n: Summary

- **0** never has an inverse
  - The Multiplicative Property of Zero holds
- **1** is always its own inverse
- **-1** in the form of (n – 1) is also always its own inverse

- A Multiplication Table in Z_n: Summary

Z_n	Have Inverse	Don't Have Inverse
12	1, **5, 7,** 11	0, **2, 3, 4, 6, 8, 9, 10**
11	1, **2, 3, 4, 5, 6, 7, 8, 9,** 10	0
10	1, **3, 7**, 9	0, **2, 4, 5, 6, 8**
9	1, **2, 4, 5, 7,** 8	0, **3, 6**
8	1, **3, 5,** 7	0, **2, 4, 6**
7	1, **2, 3, 4, 5,** 6	0
6	1, 5	0, **2, 3, 4**
5	1, **2, 3,** 4	0

Modular Arithmetic

- A Multiplication Table in Z_n: Summary
  - The numbers that have inverses in Z_n are **relatively prime** to n
    - That is: gcd(x, n) = 1
  - The numbers that do NOT have inverses in Z_n have **common prime factors** with n
    - That is: gcd(x, n) > 1

Modular Arithmetic

- A Multiplication Table in Z_n: Summary
  - The results have implications for division:
    - Some divisions have no answers
      - 3 * x = 2 mod 6 has no solutions => 2/3 has no equivalent in Z_6
    - Some division have multiple answers
      - 2 * 2 = 4 mod 6 => 4/2 = 2 mod 6
      - 2 * 5 = 4 mod 6 => 4/2 = 5 mod 6
    - Only numbers that are **relatively prime** to n will be uniquely divisible by all elements of Z_n

Modular Arithmetic

- A Multiplication Table in Z_n: Summary
  - The results have implications for division:
    - Zero divisors exist in some mods:
    - 3 * 2 = 0 mod 6 => 0/3 = 2 and 0/2 = 3 in mod 6
    - 3 * 6 = 0 mod 9 => 0/3 = 6 and 0/6 = 3 in mod 9

Extended Euclidean Algorithm

- calculates not only GCD but x & y:

  $$ax + by = d = \gcd(a, b)$$

- useful for later crypto computations
- follow sequence of divisions for GCD but assume at each step i, can find x &y:

  $$r = ax + by$$

- at end find GCD value and also x & y
- if GCD(a,b)=1 these values are inverses

Finding Inverses

```
EXTENDED EUCLID(m, b)
1. (A1, A2, A3)=(1, 0, m);
   (B1, B2, B3)=(0, 1, b)
2. if B3 = 0
   return A3 = gcd(m, b); no inverse
3. if B3 = 1
   return B3 = gcd(m, b); B2 = b^-1 mod m
4. Q = A3 div B3
5. (T1, T2, T3)=(A1 - Q B1, A2 - Q B2, A3 - Q B3)
6. (A1, A2, A3)=(B1, B2, B3)
7. (B1, B2, B3)=(T1, T2, T3)
8. goto 2
```

Example

How to find the inverse of 550 in GF(1759), let us use a = 1759 and b = 550 and solve for 1759x + 550y = gcd(1759, 550). The results are shown in Table on next slide

Thus, we have

$$1759 \times (-111) + 550 \times 355$$
$$= -195249 + 195250 = 1.$$

Inverse of 550 in GF(1759)

Q	A1	A2	A3	B1	B2	B3
—	1	0	1759	0	1	550
3	0	1	550	1	–3	109
5	1	–3	109	–5	16	5
21	–5	16	5	106	–339	4
1	106	–339	4	–111	355	1

From above results ; we have

1759 x (–111) + 550 x 355 = –195249 + 195250 = 1.

Finding Inverses in Z_n

- The numbers that have inverses in Z_n are **relatively prime** to n
- We can use the Euclidean Algorithm to see if a given "x" is relatively prime to "n"; then we know that an inverse does exist.
- How can we find the inverse without looking at all the remainders? A problem for large n.

Finding Inverses in Z_n

- Convert $1 = x * 26 + y * 15$ to mod 26 and we get:
- $1 \bmod 26 \equiv (y * 15) \bmod 26$
- Then if we find y we find the inverse of 15 in mod 26.
- So we start from 1 and work backward…

Alternative method for finding Modular Inverse

- Using the Extended Euclidean Algorithm
  - Formalizing the backward steps we get this formula:
    - $y_0 = 0$
    - $y_1 = 1$
    - $y_i = (y_{i-2} – [y_{i-1} * q_{i-2}]); i > 1$
  - Related to the “Magic Box” method

Modular Arithmetic

Step 0	26 = 1 * 15 + 11	$y_0 = 0$
Step 1	15 = 1 * 11 + 4	$y_1 = 1$
Step 2	11 = 2 * 4 + 3	$y_2 = (y_0 – (y_1 * q_0))$ $= 0 – 1 * 1 \bmod 26 = 25$
Step 3	4 = 1 * 3 + 1	$y_3 = (y_1 – (y_2 * q_1))$ $= 1 – 25 * 1 = -24 \bmod 26 = 2$
Step 4	3 = 3 * 1 + 0	$y_4 = (y_2 – (y_3 * q_2))$ $= 25 – 2 * 2 \bmod 26 = 21$
Step 5	Note: q_i is in red above	$y_5 = (y_3 – (y_4 * q_3))$ $= 2 – 21 * 1 = -19 \bmod 26 =$ **7**

Modular Arithmetic

- Using the Extended Euclidean Algorithm
  - $y_0 = 0$
  - $y_1 = 1$
  - $y_i = (y_{i-2} - [y_{i-1} * q_{i-2}]); i > 1$
- Try it for…
  - 13 mod 22
  - 17 mod 97

Modular Arithmetic

- Using the Extended Euclidean Algorithm
  - 22 = 1 * 13 + 9 y[0]=0
  - 13 = 1 * 9 + 4 y[1]=1
  - 9 = 2 * 4 + 1 y[2]=0 - 1 * 1 mod 22 = 21
  - 4 = 4 * 1 + 0 y[3]=1 - 21 * 1 mod 22 = 2
  - Last Step : y[4]=21 - 2 * 2 mod 22 = 17

  - Check: 17 * 13 = 221 = 1 mod 22

Modular Arithmetic

- Using the Extended Euclidean Algorithm
  - 97 = 5 * 17 + 12 x[0]=0
  - 17 = 1 * 12 + 5 x[1]=1
  - 12 = 2 * 5 + 2 x[2]=0 - 1 * 5 mod 97 = 92
  - 5 = 2 * 2 + 1 x[3]=1 - 92 * 1 mod 97 = 6
  - 2 = 2 * 1 + 0 x[4]=92 - 6 * 2 mod 97 = 80
  - Last Step: x[5]=6 - 80 * 2 mod 97 = 40

  - Check: 40 * 17 = 680 = 1 mod 97

Prime Factorisation

- to **factor** a number n is to write it as a product of other numbers: $n=a \times b \times c$
- note that factoring a number is hard compared to multiplying the factors together to generate the number
- the **prime factorisation** of a number n is when its written as a product of primes
  - eg. $91=7\times13$; $3600=24\times32\times52$

$$a = \prod_{p \in \mathrm{P}} p^{a_p}$$

EULER'S TOTIENT FUNCTION

$\phi(n)$ is the number of non-negative integers less than n which are relatively prime to n.

n	$\phi(n)$	n	$\phi(n)$	n	$\phi(n)$
1	0	10	4	19	18
2	1	11	10	20	8
3	2	12	4	21	12
4	2	13	12	22	10
5	4	14	6	23	22
6	2	15	8	24	8
7	6	16	8	25	20
8	4	17	16	26	12
9	4	18	6	27	18

Some Important Values of $\phi(n)$:

n	$\phi(n) =$	Conditions
p	$p-1$	p prime
p^n	$p^n - p^{n-1}$	p prime
$s \cdot t$	$\phi(s) \cdot \phi(t)$	$\gcd(s,t) = 1$
$p \cdot q$	$(p-1) \cdot (q-1)$	p, q prime

Fermat's Little Theorem: If p is prime and $p \nmid a$ then $a^{p-1} \equiv 1 \bmod p$.

a	$a^6 \bmod 7$
2	$2^6 = 64 \equiv 1 \bmod 7$
3	$3^6 = 729 \equiv 1 \bmod 7$
4	$4^6 = 4,096 \equiv 1 \bmod 7$
5	$5^6 = 15,6251 \equiv 1 \bmod 7$

–where p is prime and $\gcd(a,p) = 1$

Euler's Theorem

- a generalisation of Fermat's Theorem
- $a^{ø(n)} \bmod n = 1$
  - where $\gcd(a,n)=1$
- eg.
  - $a=3; n=10;\ ø(10)=4;$
  - hence $3^4 = 81 = 1 \bmod 10$
  - $a=2; n=11;\ ø(11)=10;$
  - hence $2^{10} = 1024 = 1 \bmod 11$

Primitive Roots

- Suppose GCD(a,n)=1
- **Euler's theorem:** If n and a are positive integers and a is relatively prime to n then , $a^{ø(n)}(mod\ n)=1$
- Consider m such that $a^m\ mod\ n=1$
  - there may exist such m < $ø(n)$
  - once powers reach m, cycle will repeat
- if smallest is m= $ø(n)$ then a is called a **primitive root**
  - the powers of a are relatively prime to n

Examples:

1. If n=7 then 3 is the primitive root for *7*

   Because powers of 3 (from 1 to 6) are 3,2,6,4,5,1 in modulo 7. Here every number (mod7) occurs except 0.

2. If n=13 then 2 is the primitive root for 13

   Because powers of 2 are 2,4,8,3,6,12,11, 9,5,10,7… every number in (mod13) occurs except 0.

Example cont…

If n=14 then

Z_{14}^{x} is the congruence classes {1,3,5,9,11,13}

Which are relatively prime to 14

Ø (14) = 6

n	n	n^2	n^3	n^4	n^5	n^6 (mod 14)
1:	1					
3:	3	9	13	11	5	1
5:	5	11	13	9	3	1
9:	9	9	11	1		
11:	11	11	9	1		
13:	13	13	1			

Hence 3 and 5 are the primitive roots (mod14)

Discrete Logarithms

- the inverse problem to exponentiation is to find the **discrete logarithm** of a number modulo p
- that is to find x where $a^x = b \bmod p$
- written as $x=\log_a b \bmod p$
- if a is a primitive root then always exists, otherwise may not
  - $x = \log_3 4 \bmod 13$ (x satisfying $3^x = 4 \bmod 13$) has no solution
  - $x = \log_2 3 \bmod 13 = 4$ by trying successive powers
- whilst exponentiation is relatively easy, finding discrete logarithms is generally a **hard** problem

Group

- a set of elements or “numbers”
  - may be finite or infinite
- with some operation whose result is also in the set (closure)
- obeys:
  - associative law: `(a.b).c = a.(b.c)`
  - has identity `e`: `e.a = a.e = a`
  - has inverses a^{-1}: $a.a^{-1} = e$
- if commutative `a.b = b.a`
  - then forms an **abelian group**

Cyclic Group

- define **exponentiation** as repeated application of operator
  - example: $a^3 = a.a.a$
- and let identity be: $e=a^0$
- a group is cyclic if every element is a power of some fixed element
  - ie $b = a^k$ for some a and every b in group
- a is said to be a generator of the group

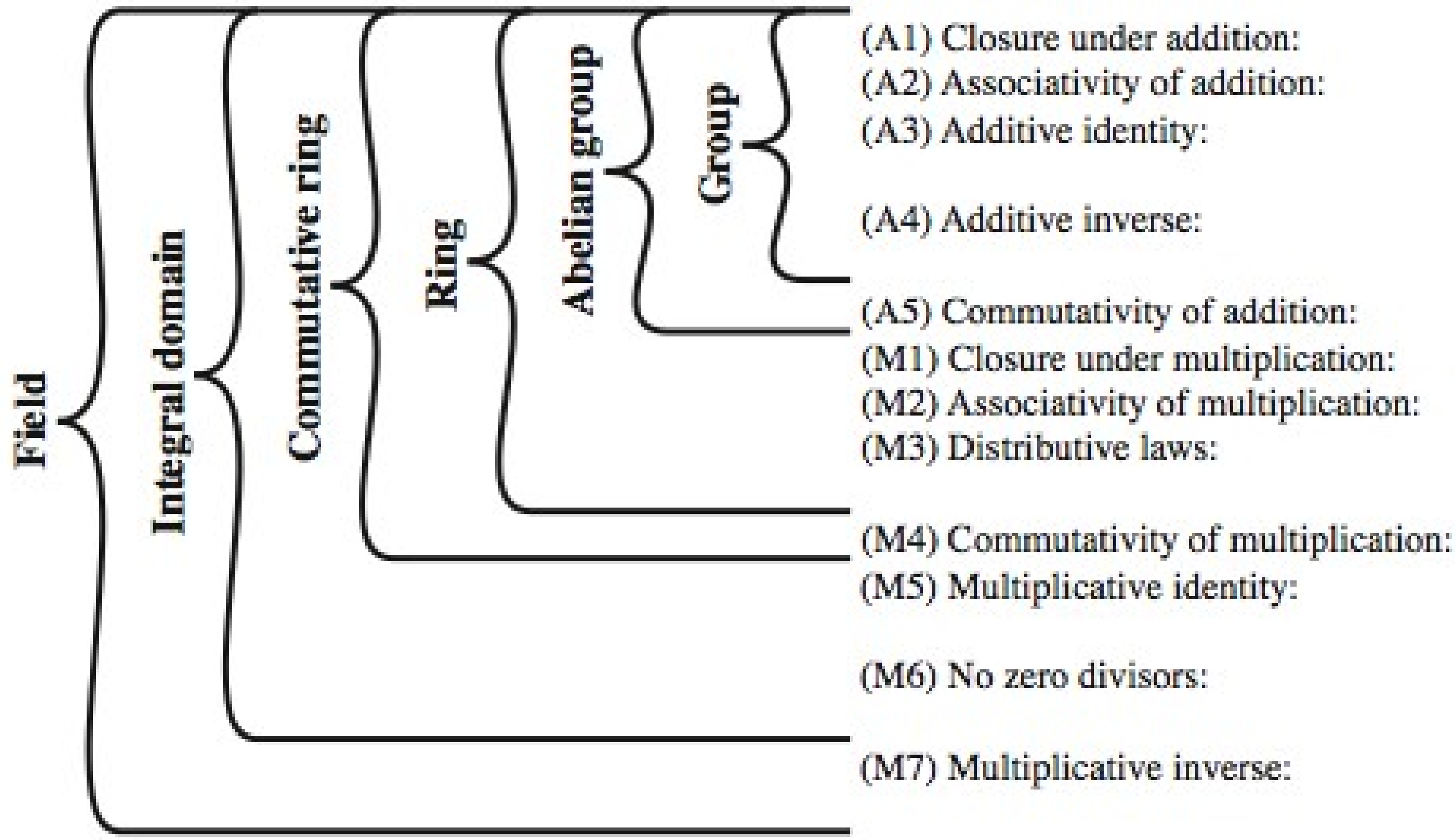
Ring

- a set of “numbers”
- with two operations (addition and multiplication) which form:
- an abelian group with addition operation
- and multiplication:
  - has closure
  - is associative
  - distributive over addition: `a(b+c) = ab + ac`
- if multiplication operation is commutative, it forms a **commutative ring**
- if multiplication operation has an identity and no zero divisors, it forms an **integral domain**

Field

- a set of numbers
- with two operations which form:
  - abelian group for addition
  - abelian group for multiplication (ignoring 0)
  - ring
- have hierarchy with more axioms/laws
  - group -> ring -> field

Group, Ring, Field



Finite (Galois) Fields

- finite fields play a key role in cryptography
- can show number of elements in a finite field **must** be a power of a prime p^n
- known as Galois fields
- denoted $GF(p^n)$
- in particular often use the fields:
  - $GF(p)$
  - $GF(2^n)$

Galois Fields GF(p)

- GF(p) is the set of integers {0,1, … , p-1} with arithmetic operations modulo prime p
- these form a finite field
  - since have multiplicative inverses
  - find inverse with Extended Euclidean algorithm
- hence arithmetic is “well-behaved” and can do addition, subtraction, multiplication, and division without leaving the field GF(p)

GF(7) Multiplication Example

×	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Polynomial Arithmetic

- can compute using polynomials

  $f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 = \sum a_i x^i$

  - nb. not interested in any specific value of x
  - which is known as the indeterminate
- several alternatives available
  - ordinary polynomial arithmetic
  - poly arithmetic with coords mod p
  - poly arithmetic with coords mod p and polynomials mod m(x)

Ordinary Polynomial Arithmetic

- add or subtract corresponding coefficients
- multiply all terms by each other
- eg

  let $f(x) = x^3 + x^2 + 2$ and $g(x) = x^2 - x + 1$

  $f(x) + g(x) = x^3 + 2x^2 - x + 3$

  $f(x) - g(x) = x^3 + x + 1$

  $f(x) \text{ x } g(x) = x^5 + 3x^2 - 2x + 2$

Polynomial Arithmetic with Modulo Coefficients

- when computing value of each coefficient do calculation modulo some value
  - forms a polynomial ring
- could be modulo any prime
- but we are most interested in mod 2
  - ie all coefficients are 0 or 1
  - eg. let $f(x) = x^3 + x^2$ and $g(x) = x^2 + x + 1$

$$f(x) + g(x) = x^3 + x + 1$$
$$f(x) \times g(x) = x^5 + x^2$$

Polynomial Division

- can write any polynomial in the form:
  - $f(x) = q(x)\, g(x) + r(x)$
  - can interpret $r(x)$ as being a remainder
  - $r(x) = f(x) \bmod g(x)$
- if have no remainder say $g(x)$ divides $f(x)$
- if $g(x)$ has no divisors other than itself & 1 say it is **irreducible** (or prime) polynomial
- arithmetic modulo an irreducible polynomial forms a field

Polynomial GCD

- can find greatest common divisor for polys
  - *c(x)* = GCD(*a(x), b(x)*) if *c(x)* is the poly of greatest degree which divides both *a(x), b(x)*
- can adapt Euclid's Algorithm to find it:

```
Euclid(a(x), b(x))
   if (b(x)=0) then return a(x);
   else return
              Euclid(b(x), a(x) mod b(x));
```

- all foundation for polynomial fields as see next

Modular Polynomial Arithmetic

- can compute in field $GF(2^n)$
  - polynomials with coefficients modulo 2
  - whose degree is less than n
  - hence must reduce modulo an irreducible poly of degree n (for multiplication only)
- form a finite field
- can always find an inverse
  - can extend Euclid's Inverse algorithm to find

Example GF(2^3)

Table 4.7 Polynomial Arithmetic Modulo ($x^3 + x + 1$)

(a) Addition

		000	001	010	011	100	101	110	111
	+	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
000	0	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
001	1	1	0	$x+1$	x	x^2+1	x^2	x^2+x+1	x^2+x
010	x	x	$x+1$	0	1	x^2+x	x^2+x+1	x^2	x^2+1
011	$x+1$	$x+1$	x	1	0	x^2+x+1	x^2+x	x^2+1	x^2
100	x^2	x^2	x^2+1	x^2+x	x^2+x+1	0	1	x	$x+1$
101	x^2+1	x^2+1	x^2	x^2+x+1	x^2+x	1	0	$x+1$	x
110	x^2+x	x^2+x	x^2+x+1	x^2	x^2+1	x	$x+1$	0	1
111	x^2+x+1	x^2+x+1	x^2+x	x^2+1	x^2	$x+1$	x	1	0

(b) Multiplication

		000	001	010	011	100	101	110	111
	×	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
000	0	0	0	0	0	0	0	0	0
001	1	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
010	x	0	x	x^2	x^2+x	$x+1$	1	x^2+x+1	x^2+1
011	$x+1$	0	$x+1$	x^2+x	x^2+1	x^2+x+1	x^2	1	x
100	x^2	0	x^2	$x+1$	x^2+x+1	x^2+x	x	x^2+1	1
101	x^2+1	0	x^2+1	1	x^2	x	x^2+x+1	$x+1$	x^2+x
110	x^2+x	0	x^2+x	x^2+x+1	1	x^2+1	$x+1$	x	x^2
111	x^2+x+1	0	x^2+x+1	x^2+1	x	1	x^2+x	x^2	$x+1$

Computational Considerations

- since coefficients are 0 or 1, can represent any such polynomial as a bit string
- addition becomes XOR of these bit strings
- multiplication is shift & XOR
  - cf long-hand multiplication
- modulo reduction done by repeatedly substituting highest power with remainder of irreducible poly (also shift & XOR)

Computational Example

- in $GF(2^3)$ have (x^2+1) is 101_2 & (x^2+x+1) is 111_2
- so addition is
  - $(x^2+1) + (x^2+x+1) = x$
  - $101 \text{ XOR } 111 = 010_2$
- and multiplication is
  - $(x+1).(x^2+1) = x.(x^2+1) + 1.(x^2+1)$

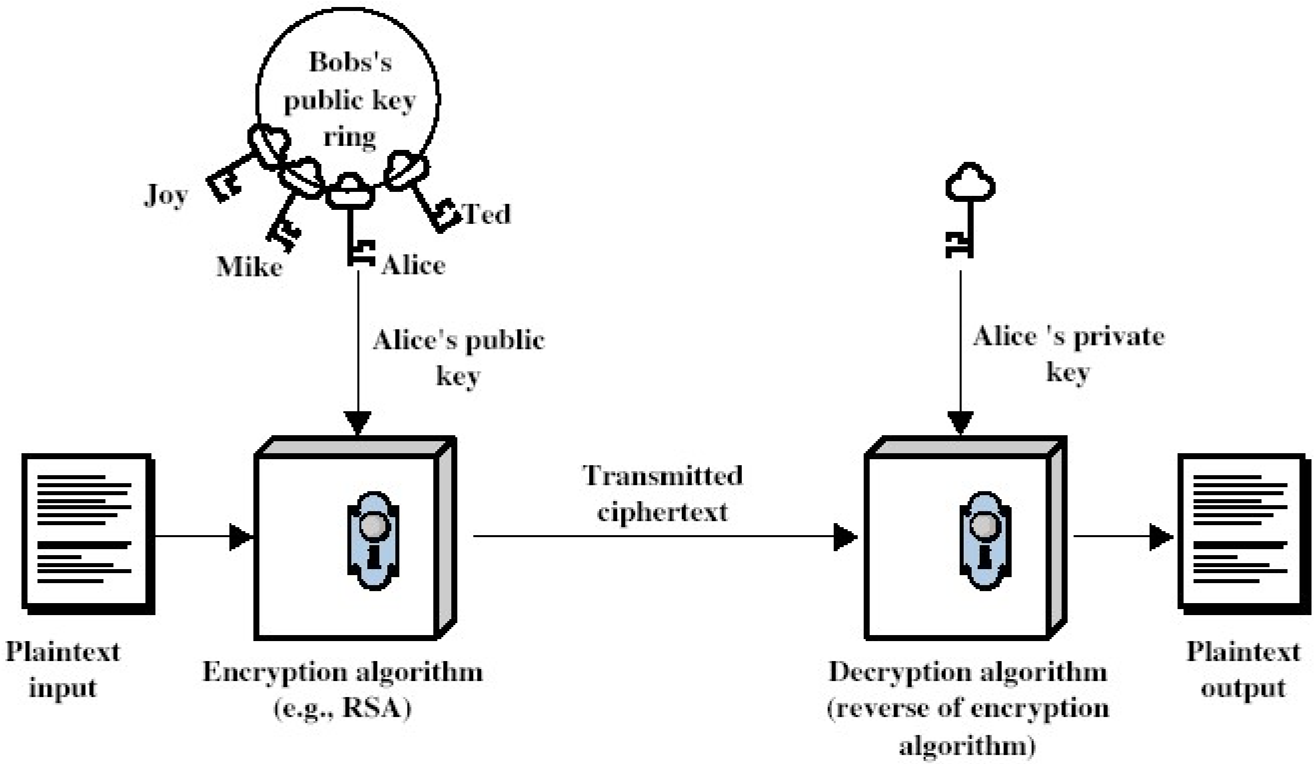
    $= x^3+x+x^2+1 = x^3+x^2+x+1$
  - $011.101 = (101) \ll 1 \text{ XOR } (101) \ll 0 =$

    $1010 \text{ XOR } 101 = 1111_2$
- polynomial modulo reduction (get q(x) & r(x)) is
  - $(x^3+x^2+x+1) \bmod (x^3+x+1) = 1.(x^3+x+1) + (x^2) = x^2$
  - $1111 \bmod 1011 = 1111 \text{ XOR } 1011 = 0100_2$

Using a Generator

- equivalent definition of a finite field
- a **generator** g is an element whose powers generate all non-zero elements
  – in F have 0, g^0, g^1, …, g^{q-2}
- can create generator from **root** of the irreducible polynomial
- then implement multiplication by adding exponents of generator

Public-Key Cryptography



TRAPDOOR

Public Key Cryptography (PKC) is based on the idea of a **trapdoor** function $f : X \to Y$, i.e.,

- f is one-to-one,
- f is easy to compute,
- f is public,
- f^{-1} is difficult to compute,
- f^{-1} becomes easy to compute if a trapdoor is known.

Thus, although in conventional cryptography the prior exchange of keys is necessary, this is not so in public key cryptography.

Public-Key Cryptography

- **public-key/two-key/asymmetric** cryptography involves the use of **two** keys:
  - a **public-key**, which may be known by anybody, and can be used to **encrypt messages**, and **verify signatures**
  - a **private-key**, known only to the recipient, used to **decrypt messages**, and **sign** (create) **signatures**
- is **asymmetric** because
  - those who encrypt messages or verify signatures **cannot** decrypt messages or create signatures

Thank You…