UNIVERSITA' DEGLI STUDI DI PARMA
Dipartimento di Ingegneria dell'Informazione

Basics of Number Theory and Modular Arithmetic

Luca Veltri
(mail.to: luca.veltri@unipr.it)

Course of Network Security, Spring 2014
http://www.tlc.unipr.it/veltri

Introduction

- Number Theory
  - **is a branch of pure mathematics devoted primarily to the study of the integers and prime numbers**
- Algebraic Number Theory
  - **branch of number theory that studies algebraic structures related to algebraic integers**
    - groups, rings, fields, etc.
      - abstract algebra
- Modular arithmetic
  - **system of arithmetic for integers, where numbers "wrap around" upon reaching a certain value (the modulus)**

Group, Ring, Field

Group

- A group is a set, G, together with an operation • (group law) that combines any two elements *a* and *b* to form another element, denoted *a•b* or *ab*
- To qualify as a group, the set and operation, {G, •}, must satisfy four requirements known as the group axioms:
  - **A1) Closure**
    - For all a,b in G, the result of the operation, a • b, is also in G
      - $(a•b) \in G, \forall\ a,b \in G$
  - **A2) Associativity**
    - For all a, b and c in G, (a • b) • c = a • (b • c)
      - $a•(b•c)=(a•b)•c, \forall\ a,b,c \in G$
  - **A3) Identity element**
    - There exists an element e in G, such that for every element a in G, the equation e • a = a • e = a holds. Such an element is unique (see below), and thus one speaks of the identity element
      - $\exists\ e : a•e=e•a=a, \forall\ a \in G$
  - **A4) Inverse element**
    - For each a in G, there exists an element b in G such that a • b = b • a = e, where e is the identity element
      - $\forall\ a \in G, \exists\ a' : a•a'=a'•a=e$

Abelian Group

- The result of an operation may depend on the order of the operands
  - **In general: $a \cdot b \neq b \cdot a$**
  - **groups for which the commutativity equation $a \cdot b = b \cdot a$ always holds are called abelian groups**
- Abelian group, also called a commutative group, is a group in which the result of applying the group operation to two group elements does not depend on their order (the axiom of commutativity)
- To qualify as an abelian group, the set and operation, {A, •}, must satisfy five requirements known as the abelian group axioms:
  - **'A' is a group (axioms 1-4)**
  - **A5) Commutativity**
    - For all a, b in A, a • b = b • a

Finite Group

- A group may have a finite or infinite number of elements
- In case the group has finite number of elements, it is called **Finite Group**
- Examples:
  - **the set of S_n of all permutations of a set of n symbols (N_n) is a group**
    - it is not an abelian group if n>2
  - **integers (>0, <0, and 0) using addition is a abelian group**
  - **real numbers (without 0) using multiplication is a abelian group**

Cyclic Group

- define **exponentiation** as repeated application of the operator
  - **$a^n = a \cdot a \cdot \ldots \cdot a$ (n times), where n is an integer**
  - **example: $a^3 = a \cdot a \cdot a$**
- and let:
  - **$e = a^0$**
  - **$a^{-n} = (a')^n$**
- Cyclic group is a group that is generated by a single element
  - **every element is a power of some fixed element**
    - i.e, $b = a^k$ for some a and every b in group
    - a is said to be a generator of the group
- Examples:
  - **integers with the addition is a cyclic group generated by the element 1**
    - note that for any integer n:
      - $n = 1+1+1+..+1 = 1 \cdot 1 \cdot \ldots \cdot 1 = (1)^n$

Ring

- A ring is a set R , {R,+, •}, equipped with binary operations + and · satisfying the following eight axioms, called the ring axioms:
  - **R is an abelian group under addition (axioms A1-A5)**
    - 0 is the addition identity element
  - **M1) R has closure under multiplication**
    - $a \cdot b \in R, \forall\ a,b \in R$
  - **M2) Operation · is associative**
    - $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all a, b, c in R
  - **M3) Multiplication distributes over addition**
    - $a \cdot (b+c) = (a \cdot b)+(a \cdot c)$, and $(b+c) \cdot a = (b \cdot a)+(c \cdot a)$, for all a, b, c in R
- A ring is a set in which we can do addition, subtraction and multiplication without leaving the set
  - **$a - b = a + (-b)$**
- Example
  - **the set of all n-square matrices over the real numbers form a ring**

Integral Domain

- If multiplication operation is commutative, it forms a Commutative Ring
  - **M4) Operation · is commutative**
    - a·b = b·a for all a,b in R
- If in a Commutative Ring the multiplication operation has identity element and no zero divisors, the Commutative Ring forms an Integral Domain
  - **M5) Multiplicative identity**
    - there is an element 1 in R such that: a · 1 = a and 1 · a = a
  - **M6) No zero divisors (cancellation of the multiplication)**
    - a·b = 0 only if a=0 or b=0, ∀ a,b,c∈ R

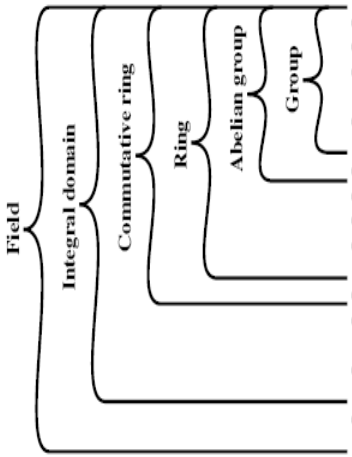
Field

- A set F together with two operations, {F,+,•}, usually called addition and multiplication, and denoted by + and •, respectively, such that the following axioms hold:
  - **F is an integral domain (axioms A1-A5, M1-M6)**
  - **M7) Multiplicative inverse**
    - for any a in F other than 0, there exists an element a^{-1} in F, such that $a \cdot (a^{-1}) = 1$
      - ∀ a∈F, ∃ a^{-1} : $a \bullet a^{-1} = (a^{-1}) \bullet a = 1$
- Subtraction and division are defined implicitly in terms of the inverse operations of addition and multiplication
  - **division is defined with the following rule:**
    - $a/b = a\,(b^{-1})$
- A field is a set in which we can do addition, subtraction, multiplication, and division without leaving the set

Field (cont.)

- Examples of fields:
  - **rational numbers, real numbers, complex numbers**
- Note:
  - **integers are NOT a field since there are no multiplicative inverses (except for 1 and -1)**

Group, Ring, and Field



(A1) Closure under addition:	If a and b belong to S, then $a + b$ is also in S
(A2) Associativity of addition:	$a + (b + c) = (a + b) + c$ for all a, b, c in S
(A3) Additive identity:	There is an element 0 in R such that $a + 0 = 0 + a = a$ for all a in S
(A4) Additive inverse:	For each a in S there is an element $-a$ in S such that $a + (-a) = (-a) + a = 0$
(A5) Commutativity of addition:	$a + b = b + a$ for all a, b in S
(M1) Closure under multiplication:	If a and b belong to S, then ab is also in S
(M2) Associativity of multiplication:	$a(bc) = (ab)c$ for all a, b, c in S
(M3) Distributive laws:	$a(b + c) = ab + ac$ for all a, b, c in S
	$(a + b)c = ac + bc$ for all a, b, c in S
(M4) Commutativity of multiplication:	$ab = ba$ for all a, b in S
(M5) Multiplicative identity:	There is an element 1 in S such that $a1 = 1a = a$ for all a in S
(M6) No zero divisors:	If a, b in S and $ab = 0$, then either $a = 0$ or $b = 0$
(M7) Multiplicative inverse:	If a belongs to S and $a \neq 0$, there is an element a^{-1} in S such that $aa^{-1} = a^{-1}a = 1$

Galois Fields

- Finite fields play a key role in cryptography
  - **all cryptographic algorithms use operations on strings of bits (that can be seen as integers)**
    - If n bits, then 2^n different values (e.g. integers from 0 to 2^n-1)
  - **In a finite field we have four operations that map elements to other elements uniformly**
- Can show number of elements in a finite field **must** be a power of a prime p:
  - **p^n**
- known as Galois fields and denoted as GF(p^n)
- in particular often use the fields:
  - **GF(p)**
  - **GF(2^n)**

Modular arithmetic and prime numbers

Modular Arithmetic

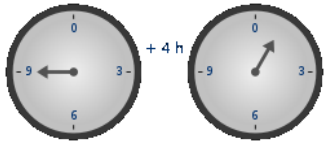
- Define **modulo operator** `a mod n` to be remainder when *a* is divided by *n*
  - **a = qn + r with: r = a mod n, 0≤r ≤ n-1, and q = a div n = ⌊a/n⌋**
- *r* is called the **residue** of *a* mod *n*
- Use the term **congruence** for: $a \equiv b \pmod n$ when divided by *n*, *a* and *b* have same remainder
- a=b (mod n) means that (a mod n) = (b mod n)
  - **eg. 100 = 34 (mod 11)**
  - **-12 mod 7 = -5 mod 7 = 2 mod 7 = 9 mod 7**
- If a=b, then a-b = 0 mod n

Modulo 7 Example

```
...
-21 -20 -19 -18 -17 -16 -15
-14 -13 -12 -11 -10  -9  -8
 -7  -6  -5  -4  -3  -2  -1
  0   1   2   3   4   5   6
  7   8   9  10  11  12  13
 14  15  16  17  18  19  20
 21  22  23  24  25  26  27
 28  29  30  31  32  33  34
...
```

Modular Arithmetic Operations

- Is 'clock arithmetic'



- Uses a finite number of values, and loops back from either end
- Modular arithmetic is when do addition & multiplication and modulo reduce the result
- Can do reduction at any point, i.e.
  - `a+b mod n = [a mod n + b mod n] mod n`
- Properties:
  - ***a*** **op** ***b*** **mod** ***n*** **≡ (*a* mod *n*) op (*b* mod *n*) = (*a* op *b*) mod *n***
  - **with op = + , - , ***

Z_n

- Z_n is defined as the set of all integers ≥0 and <n
  - $Z_n = \{0, 1, \ldots, n-1\}$
- Called set of remainders mod *n*, or set of classes of remainders mod *n*
  - **[0], [1], .., [n-1], where [r]={a : a=r mod n}, are the classes of reminders**
- Z_n form a commutative ring for addition with a multiplicative identity
- Note some peculiarities
  - **if `(a+b)≡(a+c) mod n` then `b≡c mod n`**
  - **but `(ab)≡(ac) mod n` then `b≡c mod n` is not always true**
    - only if `a` is relatively prime to `n`

Example – Arithmetic modulo 8

Addition modulo 8

+	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

Multiplication modulo 8

×	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

Additive and multiplicative inverses modulo 8

w	$-w$	w^{-1}
0	0	–
1	7	1
2	6	–
3	5	3
4	4	–
5	3	5
6	2	–
7	1	7

Properties of modular arithmetic in Z_n

Property	Expression
Commutative laws	$(w + x) \bmod n = (x + w) \bmod n$ $(w \times x) \bmod n = (x \times w) \bmod n$
Associative laws	$[(w + x) + y] \bmod n = [w + (x + y)] \bmod n$ $[(w \times x) \times y] \bmod n = [w \times (x \times y)] \bmod n$
Distributive laws	$[w \times (x + y)] \bmod n = [(w \times x) + (w \times y)] \bmod n$ $[w + (x \times y)] \bmod n = [(w + x) \times (w + y)] \bmod n$
Identities	$(0 + w) \bmod n = w \bmod n$ $(1 \times w) \bmod n = w \bmod n$
Additive inverse ($-w$)	For each $w \in Z_n$, there exists a z such that $w + z \equiv 0 \bmod n$

Divisors

- Say a non-zero number b **divides** a if for some m have $a=mb$ (a,b,m all integers)
  - **that is b divides into a with no remainder**
  - **denote this $b|a$**
  - **and say that b is a divisor of a**
- Example
  - **all of 1,2,3,4,6,8,12,24 divide 24**

Prime Numbers

- prime numbers only have divisors of 1 and self
  - **they cannot be written as a product of other numbers**
  - **note: 1 is prime, but is generally not of interest**
- eg. 2,3,5,7 are prime, 4,6,8,9,10 are not
- prime numbers are central to number theory
- list of prime number less than 200 is:

```
2 3 5 7 11 13 17 19 23 29 31 37 41 43 47 53 59 61 67 71 73 79 83 89
97 101 103 107 109 113 127 131 137 139 149 151 157 163 167 173 179
181 191 193 197 199
```


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 relatively 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.** $91=7\times13$; $3600=2^4\times3^2\times5^2$

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

Relatively Prime Numbers

- Two numbers a,b are **relatively prime** if have **no common divisors** apart from 1
- Example
  - 8 & 15 are relatively prime since factors of 8 are 1,2,4,8 and of 15 are 1,3,5,15 and 1 is the only common factor

Greatest Common Divisor (GCD)

- A common problem in number theory
- GCD of a and b, that is GCD(a,b), is the largest number that divides both a and b
  - eg GCD(60,24) = 12
- Conversely can determine the greatest common divisor by comparing their prime factorizations and using least powers
  - Example
    - $300=2^1\times3^1\times5^2$ $18=2^1\times3^2$ hence $GCD(18,300)=2^1\times3^1\times5^0=6$
- Often want **no common factors** (except 1)
  - hence numbers are relatively prime
  - e.g. GCD(8,15) = 1
    - 8 & 15 are relatively prime

Euclid's GCD Algorithm

- an efficient way to find the GCD(a,b)
- uses theorem that:
  - **GCD(a,b) = GCD(b, a mod b)**
- **Euclid's Algorithm** to compute GCD(a,b):
  - **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)
```


Multiplicative inverse (modulo *n*)

- the multiplicative inverse of a number x is the number we multiply x by to get 1
  - **with real numbers this is just 1/x**
  - **the multiplicative inverse of *m mod n* is *u : u*m = 1 (mod n)***
    - u*m differs from 1 by a multiple of n, or
      u*m + v*n = 1
- A number *m* has a multiplicative inverse m^{-1} (mod *n*) if (and only if) m and *n* are relative prime
- The Extended Euclid's Algorithm can be used to find the multiplicative inverse
  - **solving the problem:**
    - Find u,v | u*m + v*n = 1

Galois Fields GF(p)

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

Example – Arithmetic in GF(7)

Addition modulo 7

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

Multiplication modulo 7

×	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

Additive and multiplicative inverses modulo 7

w	$-w$	w^{-1}
0	0	–
1	6	1
2	5	4
3	4	5
4	3	2
5	2	3
6	1	6

Extended Euclid's Algorithm

$r_{-1} \leftarrow n$; $r_0 \leftarrow m$
$a_{-1} \leftarrow 1$; $a_0 \leftarrow 0$
$b_{-1} \leftarrow 0$; $b_0 \leftarrow 1$
$k \leftarrow 0$
while $(r_k \neq 0)$ **do**
  $q_{k+1} \leftarrow \lfloor r_{k-1}/r_k \rfloor$
  $r_{k+1} \leftarrow r_{k-1} \ \% \ r_k$
  $a_k \leftarrow a_{k-2} - q_k a_{k-1}$
  $b_k \leftarrow b_{k-2} - q_k b_{k-1}$
  $k \leftarrow k+1$
endwhile
return r_{k-1}

For each k ≥ -1 :

$$r_k = a_k n + b_k m$$

At the end:

$$r_{k-1} = (n,m) = \lambda n + \mu m$$

The number of iteration is:
$\mathcal{O}(\log(m))$

The algorithm always ends due to:
$r_0 > r_1 > r_2 > \cdots \geq 0$

Extended Euclid's Algorithm (cont.)

k	q_k	r_k	a_k	b_k	
−1		43	1	0	
0		35	0	1	
1	43 = 1 · 35 +	8	1	−1	8 = 1 · 43 + (−1) · 35
2	35 = 4 · 8 +	3	−4	5	3 = (−4) · 43 + 5 · 35
3	8 = 2 · 3 +	2	9	−11	2 = 9 · 43 + (−11) · 35
4	3 = 1 · 2 +	1	−13	16	1 = (−13) · 43 + 16 · 35
5	2 = 2 · 1 +	0			

- Algorithm start with k=1
- At each step the new coefficients r_k, q_k are calculated:
  - $q_k = \lfloor r_{k-2} / r_{k-1} \rfloor$
  - $r_k = r_{k-2} \bmod r_{k-1}$
  - that is: $r_k = r_{k-2} - q_k r_{k-1}$
- From r_k, e q_k , the new values of a_k e b_k are calculated:
  - $a_k = a_{k-2} - q_k a_{k-1}$
  - $b_k = b_{k-2} - q_k b_{k-1}$

Fermat's Theorem

- $a^{p-1} \bmod p = 1$
  - **where p is prime and gcd(a,p)=1**
- also known as Fermat's Little Theorem

Euler Totient Function ø(n)

- When doing arithmetic modulo n
- **Complete set of residues** is: 0..n-1
- **Reduced set of residues** is those numbers (residues) which are relatively prime to n
  - **eg for n=10,**
  - **complete set of residues is {0,1,2,3,4,5,6,7,8,9}**
  - **reduced set of residues is {1,3,7,9}**
- Number of elements in reduced set of residues is called the **Euler Totient Function ø(n)**

Euler Totient Function ø(n)

- To compute ø(n) need to count number of elements to be excluded
- In general need prime factorization, but
  - **for p (p prime)** $\phi(p) = p-1$
  - **for p.q (p,q prime)** $\phi(p.q) = (p-1)(q-1)$
- Examples
  - $\phi(37) = 36$
  - $\phi(21) = (3-1)\times(7-1) = 2\times6 = 12$

Euler's Theorem

- A generalization of Fermat's Theorem
- $a^{\phi(n)} \bmod n = 1$
  - **where gcd(a,n)=1**
- e.g.
  - **a=3;n=10; ø(10)=4;**
  - **hence $3^4 = 81 = 1 \bmod 10$**
  - **a=2;n=11; ø(11)=10;**
  - **hence $2^{10} = 1024 = 1 \bmod 11$**
- Corollary from Eulers's Theorem
  - **$a^{k\phi(n)+1} \bmod n = a$**

Primitive Roots

- from Euler's theorem have $a^{\phi(n)} \bmod n = 1$
- consider $a^m \bmod n = 1$, $GCD(a,n) = 1$
  - **must exist for m= ø(n) but may be smaller**
  - **once powers reach m, cycle will repeat**
- if smallest is m= ø(n) then a is called a **primitive root**
- if p is prime, then successive powers of a "generate" the group $\bmod p$
- these are useful but relatively hard to find

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
  - **Examples**
    - $x = \log_3 4 \bmod 13$ (x st $3^x = 4 \bmod 13$) has no answer
    - $x = \log_2 3 \bmod 13 = 4$ by trying successive powers
- whilst exponentiation is relatively easy, finding discrete logarithms is generally a **hard** problem