CS557: Cryptography

Elementary Number Theory II

S. Tripathy
IIT Patna

Previous Class

- Elementary Number Theory
  - Arithmetic
  - Time Complexity Bit operation
  - GCD
    - Euclidean Algorithm.

Present Class

- Elementary Number Theory
  - Prime number
  - Group theory
    - Group
    - Field
  - Modular Arithmetic
  - Finite Field

Find GCD (198,168)

GCD(198,168)=
GCD(168,30)=
GCD(30,18)=
GCD(18,12)=
GCD(12,6)=
GCD(6,0)=6.

Prime and composites

- An integer $n > 1$ is prime if the only positive divisors of n are 1 and n.
  - First few primes of N

    2, 3, 5, 7, 11, 13, 17, 19, 23, ... ,
  - First few composites are

    4, 6, 8, 9, 10, 12, 14, 15, 16, ...
- Prime numbers have significant importance
  - For every number x, there is a unique set of primes {p1, …,pn} and a unique set of positive exponents {e1, …,en} such that
    - $X = p_1^{e1} * p_2^{e2} \ldots * p_n^{en}$

Numbers Factor as Products of Primes

- Every natural number factors as a product of primes.
- Example:

$$\text{Let } n = 1275$$

$$n = 3 \cdot 425$$

$$n = 3 \cdot 5 \cdot 85$$

$$n = 3 \cdot 5^2 \cdot 17$$

The prime factorization of 1275

Open Problem

Is there an algorithm that can factor any integer n in polynomial time?

- Peter Shor devised a polynomial time algorithm
- Note that in 2001 IBM researchers built a quantum computer that used Shor's algorithm to factor 15

- When the numbers are very large, no efficient, non-quantum integer factorization algorithm is known
  - Not all numbers of a given length are equally hard to factor. The hardest instances of these problems (for currently known techniques) are semiprimes, the product of two prime numbers.

Open Problem

- RSA-576: Until recently there was a $10,000 bounty on factoring the following 174-digit integer

1881988129206079638386972394616504398071635633794173827007633564229888597152346654853190606065047430453173880113033967161996923212057340318795506569962213051687593076502570 59

- It was factored at the German Federal Agency for Information Technology Security in December 2003

398075086424064937397125500550386491199064362342
526708406385189575946388957261768583317

×

472772146107435302536223071973048224632914695302
097116459852171130520711256363590397527

Open Problem

- The next RSA challenge is RSA-640:

3107418240490043721350750035888567930037346022842727
54572016194882320644051808150455634682967172328678243
79162728380334154710731085019195485290073377248227835
25742386454014691736602477652346609

- Its factorization was worth $20,000 until November 2005 when it was factored by F. Bahr, M. Boehm, J. Franke, and T. Kleinjun. This factorization took five months

- Here is one of the prime factors (you can find the other):

1634733645809253848443133883865090859841783670033092
312181110852389333100104508151212118167511579

(This team also factored a 663-bit RSA challenge integer.)

Open Problem

- RSA-768 has 232 decimal digits (768 bits), and was factored on December 12, 2009 over the span of 2 years, by Thorsten Kleinjung, et.al.
- The CPU time spent on finding these factors by a collection of parallel computers amounted approximately to the equivalent of almost 2000 years of computing on a single-core 2.2 GHz AMD Opteron-based computer
- RSA-768 =
  1230186684530117755130494958384962720772853569595334792197322452151726400572636575187452021997864693899564749427740638459251925573263034537315482685079170261221429134616704292143116022212404792747377940806653514195974598569021 43413
- =33478071698956898786044169848212690817704794983713768568912431388982883793780022876147116525317430877378144679994 89 ×
  3674604366679959042824463379962795263227915816434308764267603228381573966651127923337341714339681027009279873630 8917

Open Problem

- RSA-896 has 896 bits (270 decimal digits), and has not been factored so far. A cash prize of $75,000 was previously offered for a successful factorization.

- RSA-896 =
412023436986659543855531365332575948179811699844327982845455626433876445565248426198098870423161841879261420247188869492560931776375033421130982397485150944909106910269861031862704114880866970564902903653658867433731720813104105190864254793282601391257624033946373269391

Sequence of Prime Numbers

- Will discuss on the following Questions
  - Are there infinitely many primes?
  - Given a, b $\in$ Z, are there infinitely many primes of the form ax + b?
  - How are the primes spaced along the number line?

Euclid Theorem

- There are infinitely many primes.
- Proof:
  - Let $p_1, p_2, \ldots, p_n$ are n distinct primes.
  - We construct a prime p_{n+1} not equal to any of p1 , ... , p_n, as follows.
  - If $N = (p_1p_2p_3 \cdots p_n) + 1$
  - then there is a factorization $N = q_1q_2 \cdots q_m$ with each q_i prime and $m \geq 1$
  - If $q_1 = p_i$ for some i, then $p_i \mid N$
  - we also have $p_i \mid N - 1$ since $N = (p_1p_2p_3 \cdots p_n) + 1$
    - which is a contradiction.
- Thus the prime $p_{n+1} = q_1$ is not in the list $p_1, \ldots, p_n$, and we have constructed our new prime.

Enumerating Primes

Algorithm (Prime Sieve)

Given a positive integer n, this algorithm computes a list of the primes up to n.

1. [Initialize] Let $X = [3, 5, \ldots]$ be the list of all odd integers between 3 and n. Let $P = [2]$ be the list of primes found so far.
2. [Finished?] Let p be the first element of X. If $p \geq \sqrt{n}$, append each element of X to P and terminate. Otherwise append p to P
3. [Cross Off] Set X equal to the sublist of elements in X that are not divisible by p. *Go to Step 2.*

Example

- To list the primes ≤ 40 using the sieve, we proceed as follows
- First

$$P = [2]$$

$$X = [3, 5, 7, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29, 31, 33, 35, 37, 39].$$

- We append 3 to P and cross off all multiples of 3 to obtain the new list

$$P = [2,3]$$

$$X = [5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35, 37].$$

- Next we append 5 to P , and cross off the multiples

$$P = [2, 3, 5]$$

$$X = [7, 11, 13, 17, 19, 23, 29, 31, 37]$$

- Because $7^2 \geq 40$, we append X to P

$$P = [2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37]$$

Group Theory Concept

Group

- An Algebraic structure has a set of elements or "numbers" with some operation <G,O>, G={a,b,c,..}, O= '.' (dot) 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*

Thm: The order of subgroup H of a finite group G divides the order of G

Examples

Is (Z,+) a group?

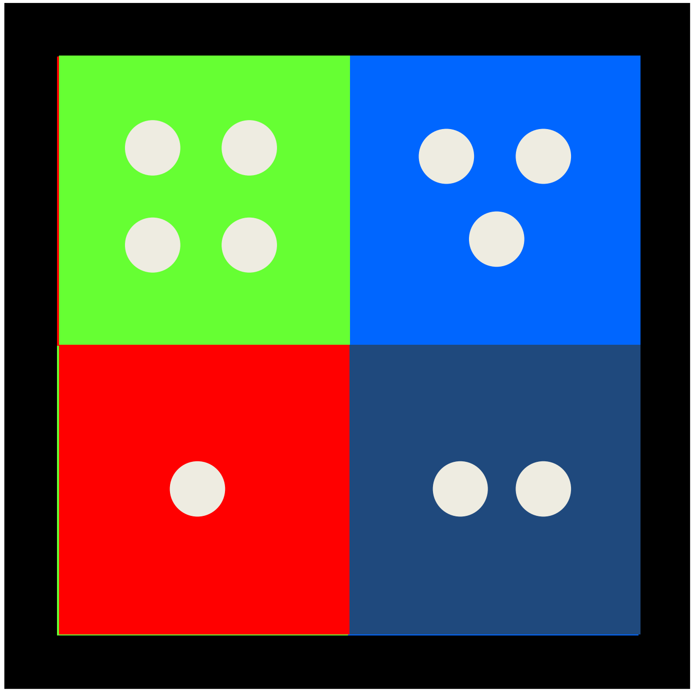
Is + associative on Z? YES!

Is there an identity? YES: 0

Does every element have an inverse? YES!

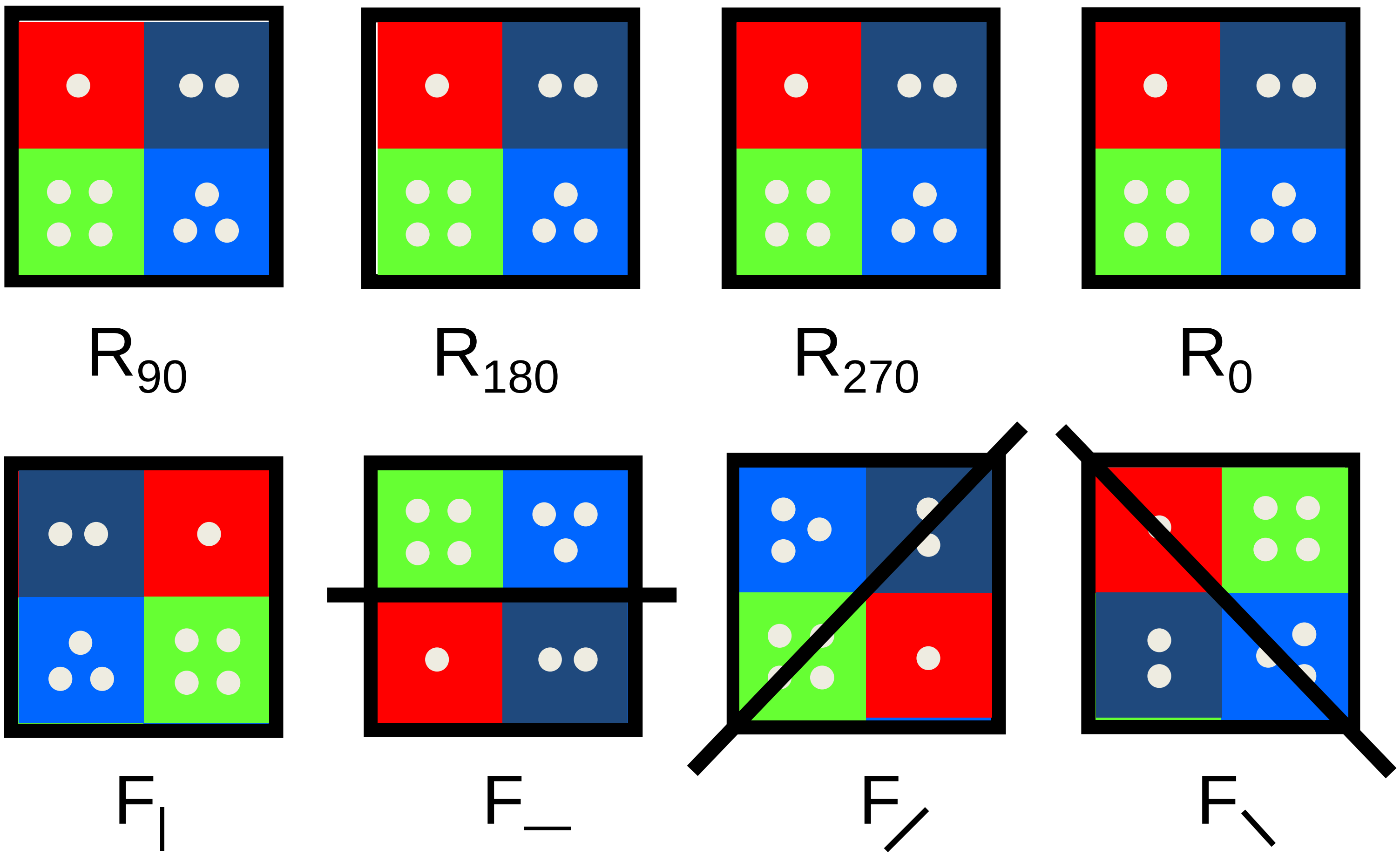
(Z,+) is a group

Rotating a Square in Space

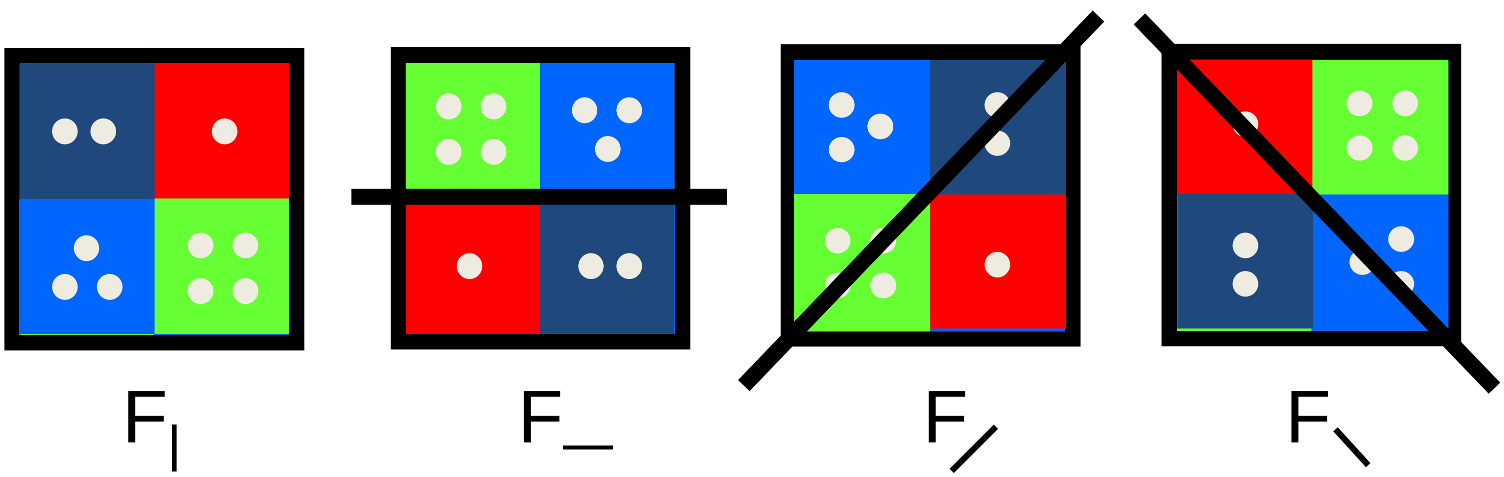


Imagine we can pick up the square, rotate it in any way we want, and then put it back on the white frame

In how many different ways can we put the square back on the frame?



We will now study these 8 motions, called symmetries of the square



Symmetries of the Square

$Y_{SQ} = \{ R_0, R_{90}, R_{180}, R_{270}, F_{|}, F_{—}, F_{\diagup}, F_{\diagdown} \}$

Composition: Define the operation "•" to mean "first do one symmetry, and then do the next"

EX. $R_{90} \bullet R_{180}$ means "first rotate 90˚ clockwise and then 180˚"

$= R_{270}$

Formally, • is a function from $Y_{SQ} \times Y_{SQ}$ to Y_{SQ}

$$\bullet : Y_{SQ} \times Y_{SQ} \to Y_{SQ}$$

Question: if $a,b \in Y_{SQ}$, does $a \bullet b \in Y_{SQ}$? Yes!

	R_0	R_{90}	R_{180}	R_{270}	$F_{\vert}$	F_{-}	$F_{/}$	$F_{\backslash}$
R_0	R_0	R_{90}	R_{180}	R_{270}	$F_{\vert}$	F_{-}	$F_{/}$	$F_{\backslash}$
R_{90}	R_{90}	R_{180}	R_{270}	R_0	$F_{\backslash}$	$F_{/}$	$F_{\vert}$	F_{-}
R_{180}	R_{180}	R_{270}	R_0	R_{90}	F_{-}	$F_{\vert}$	$F_{\backslash}$	$F_{/}$
R_{270}	R_{270}	R_0	R_{90}	R_{180}	$F_{/}$	$F_{\backslash}$	F_{-}	$F_{\vert}$
$F_{\vert}$	$F_{\vert}$	$F_{/}$	F_{-}	$F_{\backslash}$	R_0	R_{180}	R_{90}	R_{270}
F_{-}	F_{-}	$F_{\backslash}$	$F_{\vert}$	$F_{/}$	R_{180}	R_0	R_{270}	R_{90}
$F_{/}$	$F_{/}$	F_{-}	$F_{\backslash}$	$F_{\vert}$	R_{270}	R_{90}	R_0	R_{180}
$F_{\backslash}$	$F_{\backslash}$	$F_{\vert}$	$F_{/}$	F_{-}	R_{90}	R_{270}	R_{180}	R_0

Examples

Is $(Y_{SQ}, \bullet)$ a group?

Is $\bullet$ associative on Y_{SQ}? YES!

Is there an identity? YES: R_0

Does every element have an inverse? YES!

$(Y_{SQ}, \bullet)$ is a group

Cyclic Group

- *exponentiation* may be defined as repeated application of operator
  - example: $a^3 = a.a.a$
- and let identity be: $e=a^0$

- *Cyclic group :* a group is cyclic if every element is a power of some fixed element
  - i.e b = g^k for some g and every b in group
- g is said to be a generator of the group

- Ex: $(Z_7^*, .)$ 3 is a generator: $3^2 = 9 \bmod 7 = 2$, $3^3 = 6$,.., $3^6 = 1 \bmod 7$, but 2 is not generator {1,2,4,8}

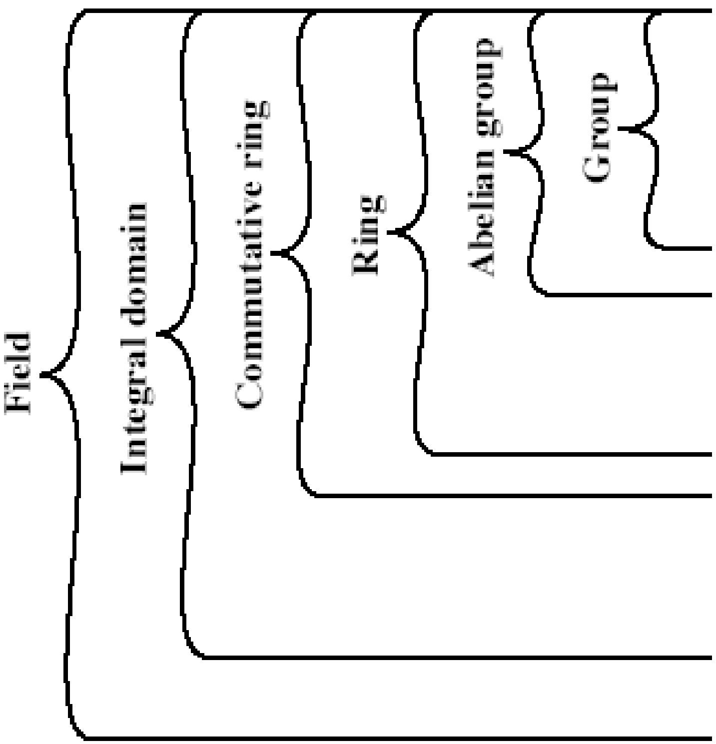
Ring

- (R,+,.) a set of "numbers" with two operations (addition and multiplication) which are:
- an abelian group with operation +
- Multiplication(.):
  - has closure
  - is associative
  - distributive over addition: a.(b+c) = a.b + a.c

- if multiplication operation is commutative, it forms a <u>*commutative ring*</u>
- if multiplication operation has identity and no zero divisors, it forms an <u>*integral domain*</u>

Field

- a set of numbers with two operations: (F,+,.)
  - abelian group for + operation
  - abelian group for . operation (ignoring 0)
  - ring



(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 0, there is an element a^{-1} in S such that $aa^{-1} = a^{-1}a = 1$