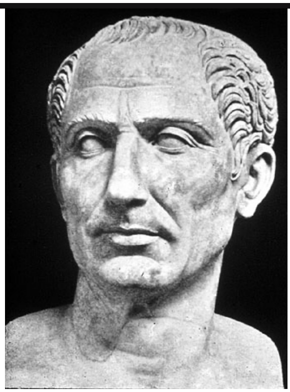
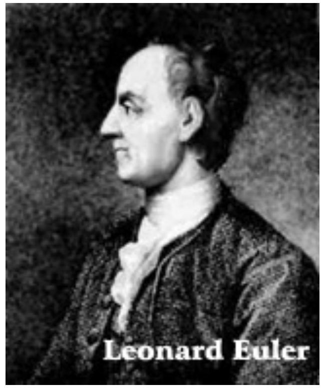
EE488
Intro to Cryptography Engineering (and Cryptocurrency)

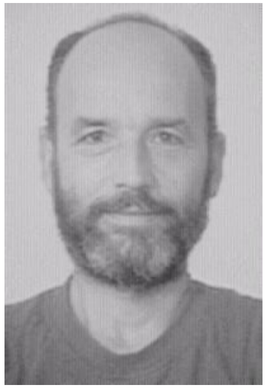
Yongdae Kim
SysSec @ KAIST

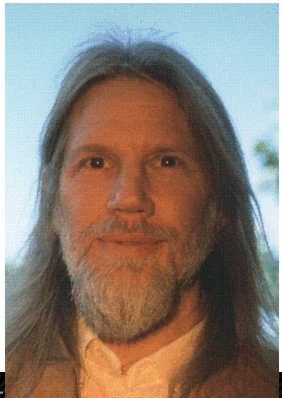
SysSec
System Security Lab

Who’s who?



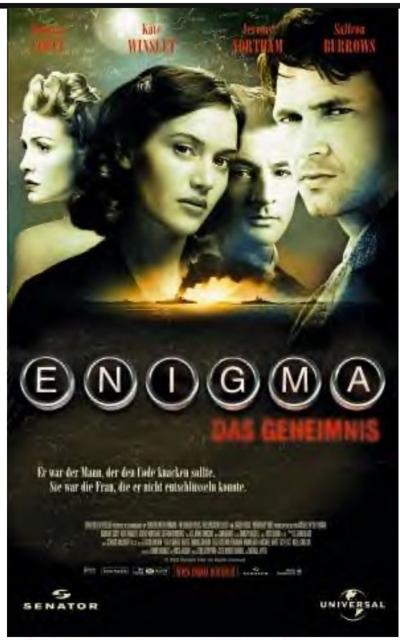



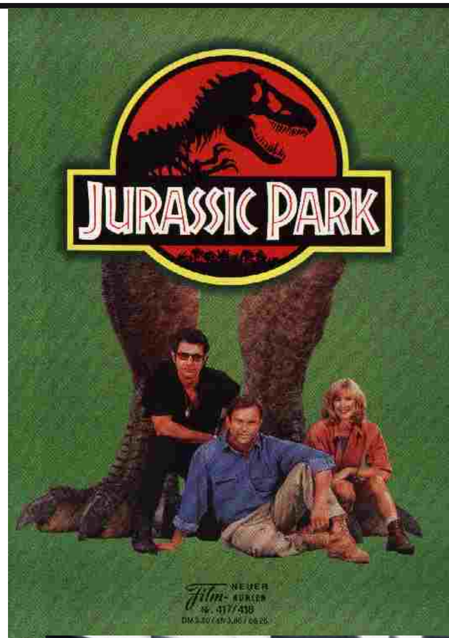



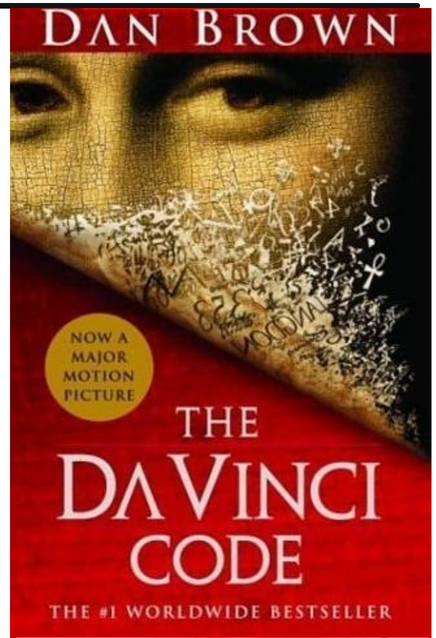


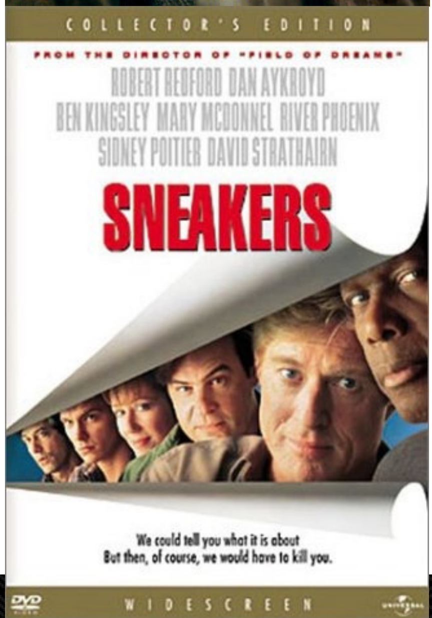
Some movies


RUSSELL CROWE
A BEAUTIFUL MIND


ENIGMA
DAS GEHEIMNIS
SENATOR
UNIVERSAL


JURASSIC PARK


DAN BROWN
NOW A MAJOR MOTION PICTURE
THE DA VINCI CODE
THE #1 WORLDWIDE BESTSELLER


COLLECTOR'S EDITION
FROM THE DIRECTOR OF "FIELD OF DREAMS"
ROBERT REDFORD DAN AYKROYD
BEN KINGSLEY MARY MCDONNEL RIVER PHOENIX
SIDNEY POITIER DAVID STRATHAIRN
SNEAKERS
We could tell you what it is about
But then, of course, we would have to kill you.
WIDESCREEN


Meet James Bond,
secret agent 007
His new incredible women...
His new incredible enemies...
His new incredible adventures...
HARRY SALTZMAN AND ALBERT R. BROCCOLI
IAN FLEMING'S
FROM RUSSIA WITH LOVE
SEAN CONNERY AS JAMES BOND
DANIELA BIANCHI
RICHARD MAIBAUM JOHANNA HARWOOD LIONEL BART JOHN BARRY
HARRY SALTZMAN ALBERT R. BROCCOLI TERENCE YOUNG
TECHNICOLOR
UNITED ARTISTS


JOHN TRAVOLTA/HUGH JACKMAN/HALLE BERRY/DON CHEADLE
Log on.
Hack in.
Go anywhere.
Steal everything.
SWORDFISH


U-571

Introduction

- Class Information
  - Title: Intro to Cryptography Engineering
  - Course Number: EE 488
  - Lectures: MW 10:30Am - 11:45Am, N1 112

- Has been experimental and challenging to teach this course…
  - Trying to learn how to teach this course well

Instructor, TA, Office Hours

- Instructor
  - Yongdae Kim
    - Taught this class 16 times in KAIST and U of Minnesota
  - Email: yongdaek(at)kaist.ac.kr, yongdaek(at)gmail.com
    - Please include [ee488] in the subject of your mail
  - Office: N26 201
  - Office Hours: By Appointment
- TA
  - Beomseok Oh, Sangmin Woo, Kwangmin Kim
  - email : ee488ta (at) syssec.kaist.ac.kr
  - Office hours: By Appointment

Class web page, e-mail

- https://syssec.kaist.ac.kr/~yongdaek/courses/ee488/
- Read the page carefully and regularly!
  - Read the Syllabus carefully.
  - Check calendar.

- KLMS

- E-mail policy
  - Include [ee488] in the subject of your e-mail

Textbook

- Handbook of Applied Cryptography by Alfred J. Menezes, Paul C. Van Oorschot, Scott A. Vanstone (Editor), CRC Press, ISBN 0849385237, (October 16, 1996) Available on-line at http://www.cacr.math.uwaterloo.ca/hac/
- Some readings from various sources

Prerequisite

- Recommended
  - Discrete Mathematics, Data Structure or Algorithm and some math

- Quiz this Wednesday
  - To understand your mathematical knowledge
  - Nothing to do with your grade

Pre Quiz Wednesday

- Not part of your grade
- Prepare an empty paper
- Write down your name and email address
- Write your answers
- Take pictures and send them to ee488ta (at) syssec.kaist.ac.kr

Course Objectives

- To learn
  - mathematical background for cryptographic techniques
  - basic cryptographic techniques for computer and network security
  - how secure these techniques are
  - **how to use these techniques securely**
  - **how to apply these techniques**

Student Expectations

- Keep up with material
  - complete relevant readings before class
  - browse lecture slides
    - Slides will be on-line the same day, after class
- Attend lectures
  - Understanding lecture is as important as reading before class.
- Feedback!!!!
- Read your email regularly. No excuses!
- Quizzes, Exams and homework:
  - LLM policy: You can use it for your homework.
  - You are encouraged to discuss with your friends.
  - But, write your own answer!
  - Violators will be prosecuted

Class Information

- Lecture format
  - Slides (will try to post before class, but not guaranteed)
- Zoom courtesy
  - Turn you camera on (if you don’t have a specific problem)
  - Turn your mic off
- Browse the course Web site often
  - check it regularly
  - news and lecture notes (in PDF, PPT) will all be there
- Please read your email!

Grading

- Distribution
  - Midterm: 24%
  - Final: 30%. (In-class)
  - 6 assignments: 12 %. (6 x 3 %) Hard
  - 4 quizzes: 24 %. (4 x 6 % each) Easy
  - Attendance: 5% (1 absent = -1%)
  - Participation: 5% (1 Good Q or A = +1%)
- Policy
  - 90.0% or above yields an A, 87.0% an A-, 83% = B+, 80% = B, 75% = B-, 70% = C+, 65% = C, 60% = C-, 55% = D, and less than 50% yields an F.
  - A+ will be curved.

Assignment

- Submission instruction
  - Type up your homework by text/pdf file.
  - Submit it through KLMS
  - Due time: 10:20 AM
  - Check Calendar.
    - » First homework due: Mar 17
    - » First quiz: Mar 22
  - No grading for late Homework/missing quizzes
    - » If you cannot submit/take it, let me know in advance.
    - » We will post the answer sheet immediately.

Course Topics - tentative

- Mathematics! Mathematics! Mathematics!
- Symmetric Ciphers
- Hash Functions and Integrity
- Public Key Encryption
- Digital Signatures
- Identification and Authentication
- Key Establishment and Management
- Cryptocurrency
  - Bitcoin, Ethereum, Consensus Algorithms

You may not be able to…

- Become expert (needs time…)
- Learn everything
- Break well-known encryption algorithm
- Wireless security, P2P security, …

- You may be able to (I hope)
  - be interested in security
  - have basic background needed to understand cryptography (number theory, …)
  - Know technologies behind cryptocurrency

Math, Math, Math!

Divisibility

- $Z = \{\cdots -2, -1, 0, 1, 2, \cdots\}$
- Let a, b be integers. Then a ***divides*** b (a|b)
  - if $\exists$ c such that b = ac.
  - 16 | 32? 16 | 0?

Proof Techniques

- $p \Rightarrow q$
  - When is this true?
  - How do you prove this?
  - What is this equivalent to?
  - Direct Proof
    - » Show that the square of an even number is an even number
      - Rephrased: if n is even, then n^2 is even
    - » Proof: Assume n is even
      - $\Rightarrow$ Thus, $n = 2k$, for some k (definition of even numbers)
      - $\Rightarrow n^2 = (2k)^2 = 4k^2 = 2(2k^2)$
      - $\Rightarrow$ As n^2 is 2 times an integer, n^2 is thus even
  - Indirect Proof (Contrapositive)
    - » If n^2 is an odd integer then n is an odd integer
      - This is equivalent to: if n is even, then n^2 is even

Proof Techniques

- If n is an integer and n^3+5 is odd, then n is even
  - Which one do we need to use?

- Proof by contradiction
  - Theorem (by Euclid): There are infinitely many prime numbers.
- Proof by cases
  - Prove that $\lfloor n/2 \rfloor \cdot \lceil n/2 \rceil = \lfloor n^2/4 \rfloor$ for all integer n.
- Existence Proof: $\exists x\ P(x)$
  - Constructive: Find a specific value of c for which P(c) is true
    - a square exists that is the sum of two other squares.
  - Nonconstructive: Show that such a c exists, but don't actually find it
    - We will see examples.

Proof Techniques

- Universal Proof: $\forall x P(x)$
- Uniqueness Proof
  - If the real number equation $5x+3=a$ has a solution then it is unique
- Induction
  - Quiz
- Prove or disprove that $n^2-79n+1601$ is a prime whenever n is a positive integer

Forwards vs. Backwards reasoning

- Example: Prove that $(a+b)/2 > \sqrt{(ab)}$ when $a \neq b$, $a>0$, and $b>0$

(Pf) $(a - b)^2 > 0$

➔ $a^2 + 2\,ab + b^2 - 4\,ab > 0$

➔ $(a+b)^2 > 4ab$

➔ $((a+b)/2)^2 > ab$

➔ $(a+b)/2 > \sqrt{(ab)}$

Divisibility

- Let a, b, c be integers.
  - a|a

    We need to find c such that a = ac.

    c = 1.
  - if a|b and b|c, then a|c

    Assume a | b and b | c.

    $\Rightarrow \exists$ integers k_1, k_2 such that $b = k_1 a$ and $c = k_2 b$

    $\Rightarrow c = k_1 k_2 a$. Since $k_1 \cdot k_2$ is an integer, a | c.

    » Which proof technique we used?
  - if a|b and a|c, then a|(bx+cy) for all $x,y \in Z$
  - if a|b and b|a, then $a = \pm b$

Quotient and remainder

- Let a, b be integers and a>0. Then, there exist unique integers q and r such that

$$b = a q + r, \quad 0 \le r < a.$$

Proof) Assume that $b \ge 0$. It is clear that $\exists$ n such that $n a > b$. Let q + 1 be the least such n. Then $(q+1) a > b \ge q a$.

Let $r=b-qa$. Then, $b\ge qa$ implies $r=b-qa\ge 0$. Finally $(q+1)a=qa+a>b$ implies that $r=b-qa<a$.

To show the uniqueness, suppose $\exists$ q_1 and r_1 such that $b=qa+r=q_1a+r_1$, $0\le r,r_1< a$. Assume $r \ge r_1$. Then $0 \ge r - r_1 < a$, and $(q-q_1)a=r-r_1$. Then $a|r-r_1$. If $r-r_1>0$, $a\le r-r_1$ (since $a|r-r_1$). (*) Therefore, $r=r_1$. Then $q = q_1$.

Exercise

- If a, b, c are nonzero integers, prove that ac | bc if and only if a | b.

- Show that for any integer n, n^2 cannot be of the form 3 k + 2.

GCD, LCM

- c is a **common divisor** of a and b if c|a and c|b
- **d = gcd(a,b)** is the largest positive integer that divides both a and b, more formally
  - d > 0
  - d | a and d | b
  - e | a and e | b implies e | d
- **lcm(a,b)** is the smallest positive integer divisible by both a and b
- lcm(a,b)=a*b/gcd(a,b)
- a and b are said to be ***relatively prime*** or ***coprime*** if gcd(a,b)=1

Existence of GCD

- Let a and b be integers (a or b is not zero). Then d = gcd (a, b) exist.
- Proof (non-constructive proof)

Let $S = \{ax + by \mid x, y \in Z\}$. Let d be the least positive integer in S. Then $d = ax_0 + by_0$.

Claim: d = gcd(a, b)

i) $d>0$

iii) $e|a$ and $e|b$, then $e|d$.

ii) $d|a$, $d|b$

Let $a = dq+r$, $0 \le r < d$. Then $r = a - qd = a - q(ax_0+by_0) = a(1-qx_0) - qby_0$. Clearly $r \in S$. And $r < d$. Since d is the least positive integer in S, r = 0.Therefore, a = dq.

- Proof (constructive proof) next page!

Existence of GCD (cnt.)

- Constructive proof (Extended Eucledean Algorithm)

$b = q_1 a + r_1, \quad 0 < r_1 < a$

$a = q_2 r_1 + r_2, \quad 0 < r_2 < r_1$

$r_1 = q_3 r_2 + r_3, \quad 0 < r_3 < r_2$

…

$r_{n-2} = q_n r_{n-1} + r_n, \quad 0 < r_n < r_{n-1}$

$r_{n-1} = q_{n+1} r_n,$ (no remainder)

Since the remainder decreases and it is an integer, it will be 0 eventually.

Claim) $r_n = \gcd(a, b)$

i) $r_n > 0$

ii) $r_n \mid a$, $r_n \mid b$

iii) $e \mid a$, $e \mid b \Rightarrow e \mid r_n$.

Example

51329 = 21 2437 + 152

2437 = 16 152 + 5

152 = 30 5 + 2

5 = 2 2 + 1

2 = 2 1 + 0

1 = 5 - 2 2

= 5 - 2 (152 - 30 * 5)

= -2 152 + 61 5

= -2 152 + 61 (2437 - 16 152)

= 61 2437 - 978 152

= 61 2437 - 978 (51329 - 21 2437)

= -978 51329 + 20599 2437

Summary

- d = gcd (a, b) ⇒ ∃ x, y such that d = a x + b y.
- gcd (a, 0) = ?

- **Euclidean Algorithm** to compute GCD
  - Input: a, b with $a \geq b$
  - Output: gcd (a, b)
  - Algorithm
    - » while $b \neq 0$
      - Set $r \leftarrow a \bmod b$, $a \leftarrow b$, $b \leftarrow r$
    - » return (a)
  - Complexity?

SysSec System Security Lab

A Few more useful stuffs

- Let $d = \gcd(a, b)$
  - $\gcd(a/d, b/d) = ?$
  - $a \mid bc$ and $d = 1 \Rightarrow ?$
  - $a \mid bc \Rightarrow (a/d) \mid c$
  - $\gcd(ma, mb) = md$ if $m > 0$
- $\gcd(n, n+1)$?
- $\gcd(a, b) = \gcd(a + kb, b)$?

Prime

- $p \geq 2$ is prime if
  - $a \mid p \Rightarrow a = \pm 1$ or $\pm p$
  - Hereafter, p is prime
- [Euclid] $p \mid ab \Rightarrow p \mid a$ or $p \mid b$
- [Euclid] There are infinite number of primes.
- *Prime number theorem:*
  - let $\pi(x)$ denote the number of prime numbers $\leq x$, then $\lim_{x \to x\, \infty} \pi(x)/(x/\ln x) = 1$
- **Euler phi function**: For $n \geq 1$, let $\phi(n)$ denote the number of integers in [1, n] which are relatively prime to n.
  - if p is a prime then $\phi(p)=p-1$
  - if p is a prime, then $\phi(p^r) = p^{r-1}(p-1)$.
  - f is multiplicative. That is if gcd(m,n)=1 then $\phi(m*n) = \phi(n) * \phi(m)$

Fundamental theorem of arithmetic

- Every positive integer greater than 1 can be uniquely written as a prime or as the product of two or more primes where the prime factors are written in order of non-decreasing size

- Examples
  - 100 = 2 * 2 * 5 * 5
  - 182 = 2 * 7 * 13
  - 29820 = 2 * 2 * 3 * 5 * 7 * 71

Pairwise relative prime

- A set of integers $a_1, a_2, \cdots a_n$ are pairwise relatively prime if, for all pairs of numbers, they are relatively prime
  - Formally: The integers $a_1, a_2, \cdots a_n$ are pairwise relatively prime if $\gcd(a_i, a_j) = 1$ whenever $1 \leq i < j \leq n$.

- Example: are 10, 17, and 21 pairwise relatively prime?
  - gcd(10,17) = 1, gcd (17, 21) = 1, and gcd (21, 10) = 1
  - Thus, they are pairwise relatively prime
- Example: are 10, 19, and 24 pairwise relatively prime?
  - Since gcd(10,24) ≠ 1, they are not

Modular arithmetic

- If a and b are integers and m is a positive integer, then a is *congruent to b modulo m* if m divides a-b
  - Notation: $a \equiv b \pmod{m}$
  - Rephrased: $m \mid a-b$
  - Rephrased: $a \bmod m = b$
  - If they are not congruent: $a \not\equiv b \pmod{m}$

- Example: Is 17 congruent to 5 modulo 6?
  - Rephrased: $17 \equiv 5 \pmod{6}$
  - As 6 divides 17-5, they are congruent
- Example: Is 24 congruent to 14 modulo 6?
  - Rephrased: $24 \equiv 14 \pmod{6}$
  - As 6 does not divide 24-14 = 10, they are not congruent

Example (World of mod n)

…	-2n	-n	0	n	2n	3n	4n	…	0
…	-2n+1	-n+1	1	n+1	2n+1	3n+1	4n+1	…	1
…	-2n+2	-n+2	2	n+2	2n+2	3n+2	4n+2	…	2
…	…	…	…	…	…	…	…	…	…
…	-n-1	-1	n-1	2n-1	3n-1	4n-1	5n-1	…	n-1

More on congruence

- Every integer is either of the form 4k, 4k+1, 4k+2, 4k+3.
- Every integer is either of the form 0 mod 4, 1 mod 4, 2 mod 4, 3 mod 4
- $y^2 - x^2 - 2 \equiv 0$ mod 4 has no solution.

- Let *a* and *b* be integers, and let *m* be a positive integer. Then $a \equiv b \pmod{m}$ if and only if *a* **mod** *m* = *b* **mod** *m*
- Example: Is 17 congruent to 5 modulo 6?
  - Rephrased: does $17 \equiv 5 \pmod{6}$?
  - 17 mod 6 = 5 mod 6
- Example: Is 24 congruent to 14 modulo 6?
  - Rephrased: $24 \equiv 14 \pmod{6}$
  - 24 mod 6 ≠ 14 mod 6

Even more on congruence

- Let *m* be a positive integer. The integers *a* and *b* are congruent modulo *m* if and only if there is an integer *k* such that $a = b + km$

- Example: 17 and 5 are congruent modulo 6
  - 17 = 5 + 2*6
  - 5 = 17 -2*6

- Let a, b, c be integers.
  - $a \equiv a \bmod n$
  - $a \equiv b \bmod n \Rightarrow b \equiv a \bmod n$
  - $a \equiv b \bmod n$ and $b \equiv c \bmod n \Rightarrow a \equiv c \bmod n$.

Even even more on congruence

- Let m be a positive integer. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a+c \equiv (b+d) \pmod{m}$ and $ac \equiv bd \pmod{m}$

- Example
  - We know that $7 \equiv 2 \pmod{5}$ and $11 \equiv 1 \pmod{5}$
  - Thus, $7+11 \equiv (2+1) \pmod{5}$, or $18 \equiv 3 \pmod{5}$
  - Thus, $7*11 \equiv 2*1 \pmod{5}$, or $77 \equiv 2 \pmod{5}$

- An integer x is congruent to one and only one of the integers 0, 1, 2, ⋯, n-1 mod n.

The Caesar cipher

- Julius Caesar used this to encrypt messages

- A function f to encrypt a letter is defined as:
  $f(p) = (p+3) \bmod 26$
  - Where p is a letter (0 is A, 1 is B, 25 is Z, etc.)

- Decryption: $f^{-1}(p) = (p-3) \bmod 26$

- This is called a substitution cipher
  - You are substituting one letter with another

Arithmetic Inverse

- Let a be an integer. a* is an arithmetic inverse of a modulo n, if a a* $\equiv$ 1 mod n.

- Suppose that gcd(a, n) =1. Then a has an arithmetic inverse modulo n.

- Suppose gcd(a, n) = 1.

  Then ax $\equiv$ ay mod n $\Rightarrow$ x $\equiv$ y mod n.

- $x^2+1 \equiv 0$ mod 8 has no solution.

Equations

- $2x \equiv 5 \bmod 3$
  - $\Rightarrow 2x \equiv 2 \bmod 3$
  - $\Rightarrow 2^* \, 2\,x \equiv 2^* \, 2 \bmod 3$
  - $\Rightarrow x \equiv 1 \bmod 3 \quad (2^* \equiv 2 \bmod 3)$
- $3x \equiv 7 \bmod 5$
  - $\Rightarrow 3x \equiv 2 \bmod 5$
  - $\Rightarrow 3^* \, 3x \equiv 3^* \, 2 \bmod 5$
  - $\Rightarrow x \equiv 4 \bmod 5 \quad (3^* \equiv 2 \bmod 5)$

Summary on Congruence

- Notation: $a \equiv b \pmod{m}$
  - Rephrased: $m \mid a-b$
  - Rephrased: $a \bmod m = b$
  - Rephrased: $a = b + mk_1$ for some integer k_1
- Every integer is either of the form
  - 4k, 4k+1, 4k+2, or 4k+3.
  - 0 mod 4, 1 mod 4, 2 mod 4, or 3 mod 4
- If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then
  - $a+c \equiv (b+d) \pmod{m}$
  - $ac \equiv bd \pmod{m}$
- Suppose that gcd(a, n) =1. Then a has an arithmetic inverse a^* modulo n, i.e. $a\, a^* \equiv a^*\, a \equiv 1 \bmod n$.

Cute Exercise

- A number is divisible by 3, if sum of the all digits is divisible by 3. Why does this work?

Z_n, Z_n^*

- $Z_n = \{0, 1, 2, 3, \cdots, n\text{-}1\}$
- $Z_n^* = \{x \mid x \in Z_n \text{ and } \gcd(x, n) = 1\}$.

- $Z_6 = \{0, 1, 2, 3, 4, 5\}$
- $Z_6{*} = \{1, 5\}$

- For a set S, |S| means the number of element in S.

- $|Z_n| = n$
- $|Z_n{*}| = \phi(n)$

Cardinality

- For finite (only) sets, cardinality is the number of elements in the set

- For finite and infinite sets, two sets A and B have the same cardinality if there is a one-to-one correspondence from A to B

Counting

- Multiplication rule
  - If there are n_1 ways to do task1, and n_2 ways to do task2
    - » Then there are $n_1 n_2$ ways to do both tasks in sequence.
  - Example
    - » There are 18 math majors and 325 CS majors
    - » How many ways are there to pick one math major and one CS major?
- Addition rule
  - If there are n_1 ways to do task1, and n_2 ways to do task2
    - » If these tasks can be done at the same time, then…
    - » Then there are n_1+n_2 ways to do one of the two tasks
  - How many ways are there to pick one math major or one CS major?
- The inclusion-exclusion principle
  - $|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|$

Permutation, Combination

- An *r*-permutation is an ordered arrangement of *r* elements of the set: P(n, r), $_nP_r$
  - How many poker hands (with ordering)?
  - P(n, r) = n (n-1)(n-2)⋯(n-r+1)

    = n! / (n-r)!
- Combination: When order does not matter⋯
  - In poker, the following two hands are equivalent:
    - » A♦, 5♥, 7♣, 10♠, K♠
    - » K♠, 10♠, 7♣, 5♥, A♦
  - The number of *r*-combinations of a set with *n* elements, where *n* is non-negative and $0 \le r \le n$ is:

    C(n, r) = n! / (r! (n-r)!)
  - $(x+y)^n$

Probability definition

- The probability of an event occurring is:
  $p(E) = |E| / |S|$
  - Where E is the set of desired events (outcomes)
  - Where S is the set of all possible events (outcomes)
  - Note that $0 \leq |E| \leq |S|$
    - Thus, the probability will always between 0 and 1
    - An event that will never happen has probability 0
    - An event that will always happen has probability 1

What's behind door number three?

- The Monty Hall problem paradox
  - Consider a game show where a prize (a car) is behind one of three doors
  - The other two doors do not have prizes (goats instead)
  - After picking one of the doors, the host (Monty Hall) opens a different door to show you that the door he opened is not the prize
  - Do you change your decision?
- Your initial probability to win (i.e. pick the right door) is 1/3
- What is your chance of winning if you change your choice after Monty opens a wrong door?
- After Monty opens a wrong door, if you change your choice, your chance of winning is 2/3
  - Thus, your chance of winning doubles if you change
  - Huh?

Assigning Probability

- S: Sample space
- p(s): probability that s happens.
  - $0 \leq p(s) \leq 1$ for each $s \in S$
  - $\sum_{s \in S} p(s) = 1$
- The function p is called probability distribution
- Example
  - Fair coin: p(H) = 1/2, p(T) = 1/2
  - Biased coin where heads comes up twice as often as tail
    - » p(H) = 2 p(T)
    - » $p(H) + p(T) = 1 \Rightarrow 3\,p(T) = 1 \Rightarrow p(T) = 1/3,\ p(H) = 2/3$

More…

- Uniform distribution
  - Each element $s \in S$ ($|S| = n$) is assigned with the probability $1/n$.
- Random
  - The experiment of selecting an element from a sample space with uniform distribution.
- Probability of the event E
  - $p(E) = \sum_{s \in E} p(s)$.
- Example
  - A die is biased so that 3 appears twice as often as others
    - » $p(1) = p(2) = p(4) = p(5) = p(6) = 1/7$, $p(3) = 2/7$
  - $p(O)$ where O is the event that an odd number appears
    - » $p(O) = p(1) + p(3) + p(5) = 4/7$.

Combination of Events

- Still
  - $p(E^c) = 1 - p(E)$
  - $p(E_1 \cup E_2) = p(E_1) + p(E_2) - p(E_1 \cap E_2)$
    - » $E_1 \cap E_2 = \emptyset \Rightarrow p(E_1 \cup E_2) = p(E_1) + p(E_2)$
    - » For all $i \neq j$, $E_i \cap E_i = \emptyset \Rightarrow p(\cup_i E_i) = \sum_i p(E_i)$

Conditional Probability

- Flip coin 3 times
  - all eight possibility are equally likely.
  - Suppose we know that the first coin was tail (Event F). What is the probability that we have odd number of tails (Event E)?
    - Only four cases: TTT, TTH, THT, THH
    - So 2/4 = 1/2.

- Conditional probability of E given F
  - We need to use F as the sample space
  - For the outcome of E to occur, the outcome must belong to $E \cap F$.
  - $p(E \mid F) = p(E \cap F) / p(F)$.

Bernoulli Trials & Binomial Distribution

- Beronoulli trial
  - an experiment with only two possible outcomes
  - i.e. 0 (failure) and 1 (success).
  - If p is the probability of success and q is the probability of failure, p + q = 1.
- A biased coin with probability of heads 2/3
  - What is the probability that four heads up out of 7 trials?

Random Variable

- A random variable is a function from the sample space of an experiment to the set of real numbers.
  - Random variable assigns a real number to each possible outcome.
  - Random variable is not variable! not random!
- Example: three times coin flipping
  - Let X(t) be the random variable that equals the number of heads that appear when t is the outcome
  - X(HHH) = 3, X(THH) = X(HTH) = X(HHT) = 2, X(TTH) = X(THT) = X(HTT) = 1, X(TTT) = 0
- The distribution of a random variable X on a sample space S is the set of pairs (r, p(X=r)) for all $r \in X(S)$
  - where p(X=r) is the probability that X takes value r.
  - p(X=3) = 1/8, p(X=2) = 3/8, p(X=1) = 3/8, p(X=0) = 1/8

Expected Value

- The expected value of the random variable X(s) on the sample space S is equal to

  $E(X) = \sum_{s \in S} p(s)\, X(s)$
- Expected value of a Die
  - X is the number that comes up when a die is rolled.
  - What is the expected value of X?
  - E(X) = 1/6 1 + 1/6 2 + 1/6 3 + ··· 1/6 6 = 21/6 = 7/2
- Three times coin flipping example
  - X: number of heads
  - E(X) = 1/8 3 + 3/8 2 + 3/8 1 + 1/8 0 = 12/8 = 3/2

Questions?

- Yongdae Kim
  - email: yongdaek@kaist.ac.kr
  - Home: http://syssec.kaist.ac.kr/~yongdaek
  - Facebook: https://www.facebook.com/y0ngdaek
  - Twitter: https://twitter.com/yongdaek
  - Google "Yongdae Kim"