Number Theory

Dr Emiliano De Cristofaro

(Slides partially prepared by Jens Groth)

Last updated, September 30, 2014

Why probability theory?

- Security definitions
  - What is the probability an attacker breaks a cryptographic scheme?
- Mathematical tools
  - Use mathematical reasoning about cryptographic schemes
- Probability theory in this module
  - Elementary but extensively used
  - If you don’t have much probability background, you’re expected to catch up this week!

Finite sets

- Sets $A = \{1,2\}$ $B = \{1,2,3,4\}$ $C = \{4\}$
- Empty set $\varnothing = \{\}$
- Subsets/supersets $A \subseteq B$
- Intersection $A \cap B = \{1,2\}$
- Disjoint sets $A \cap C = \varnothing$
- Union $A \cup C = \{1,2,4\}$
- Relative complement $B \backslash A = \{3,4\}$
- Cartesian product $A \times C = \{(1,4),(2,4)\}$
- Cardinality $|A| = 2$, $|\varnothing| = 0$
- Rules $|A \cup B| = |A|+|B|-|A \cap B|$

Probability mass

- Sample space $\Omega = \{a,b,\ldots,z\}$
- Probability mass function
  - Pr: $\Omega \to [0;1]$
  - $Pr(a) + Pr(b) + \ldots + Pr(z) = 1$
- Uniform distribution
  - All samples have equal probability mass $Pr(a) = Pr(b) = \ldots = Pr(z)$
- Example
  - A die should have roughly 1/6 chance of landing on either side

Events

- Event $A \subseteq \Omega$
- Define $\Pr[A] = \sum_{x \in A} \Pr(x)$
- Immediate consequences
  - $\Pr[\varnothing] = 0$
  - $\Pr[\Omega] = 1$
  - $0 \le \Pr[A] \le 1$
- Define A and B independent events if

$$\Pr[A \cap B] = \Pr[A] \Pr[B]$$

Various rules

- If $A \subseteq B$ then $\Pr[A] \le \Pr[B]$
- $\Pr[A \cap B] \le \min(\Pr[A], \Pr[B])$
- $\max(\Pr[A], \Pr[B]) \le \Pr[A \cup B] \le \Pr[A] + \Pr[B]$
- $\Pr[A \cup B] = \Pr[A] + \Pr[B] - \Pr[A \cap B]$
- $\Pr[A] - \Pr[B] \le \Pr[A \setminus B] \le \Pr[A]$

- Homework for next week:
  – Prove them

Conditional probability

- For B with Pr[B] > 0 define

$$\Pr[A|B] = \Pr[A \cap B] / \Pr[B]$$

- Theorem: A and B are independent if and only if Pr[A|B] = Pr[A]

- Bayes theorem:

$$\Pr[A|B] = \Pr[B|A] \Pr[A] / \Pr[B]$$

Stochastic variables

- Random variable $X: \Omega \rightarrow R$
- Define

$$\Pr[X = y] = \Pr[X^{-1}(y)]$$

- Random variables

$$X: \Omega \rightarrow R,\ Y: \Omega \rightarrow S$$

  give the natural joint random variable

$$(X,Y): \Omega \rightarrow R \times S$$

- Independent random variables if for all x,y

$$\Pr[(X,Y)=(x,y)] = \Pr[X=x] \Pr[Y=y]$$

Dependent stochastic variables

- $X: \Omega \rightarrow R$, $Y: \Omega \rightarrow S$

- Properties
  - $\Pr[X=x|Y=y] = \Pr[(X,Y)=(x,y)] / \Pr[Y=y]$
  - $\Pr[X=x,Y=y] = \Pr[X=x|Y=y] \Pr[Y=y]$
- Useful observation
  - $\Pr[X=x|Y=y]\Pr[Y=y]+\Pr[X=x|Y\neq y]\Pr[Y\neq y] = \Pr[X=x]$
- Union bound
  - $\Pr[X=x \text{ or } Y=y] \leq \Pr[X=x] + \Pr[Y=y]$

Why number theory?

- Public key crypto builds on number theory!
- Number theory in this module
  - Elementary but extensively used, will be in the exam
  - You’re expected to catch up on number theory by next week!

Prime numbers

- We write $a|b$ if $b = ax$ for some $x \in \mathbf{Z}$
- A natural number N is prime if:
  - Only divisors are 1 and N
  - Examples: 2, 3, 5, 7, 11, 13, 17, 19, …
- If p is a prime and $p|ab$ then $p|a$ or $p|b$
- Any natural number N has unique prime factorization $N = p_1^{r_1} p_2^{r_2} \ldots p_s^{r_s}$

Modular reduction

- Given integers x,y we can find unique r,s such that

  $$y = sx+r$$

  with $r \in \{0,1,\ldots,x-1\}$
- We write

  $$z \equiv y \bmod x$$

  when

  $$z-y = sx$$
- If $y = sx+r$ then $y = r \bmod x$

Greatest common divisor

- Greatest common divisor of a and b is the largest number that divides both a and b
- We define $\gcd(a,b) = \max\{d : d|a \text{ and } d|b\}$
- Note, $\gcd(p,a) \in \{1,p\}$ when p is prime
- Theorem:
  - For all a,b there are r,s so that $\gcd(a,b)=ra+sb$
  - If $c|ab$ and $\gcd(a,c)=1$ then $c|b$
  - If $a|N$ and $b|N$ and $\gcd(a,b)=1$ then $ab|N$

- Theorem:
  For all a,b there are r,s so gcd(a,b)=ra+sb

- Proof:
  Define min = min({ra+sb|ra+sb>0})
  - gcd ≤ min
    - gcd|a and gcd|b so gcd|ra+sb so gcd|min
  - min ≤ gcd
    - If min|a and min|b then clear min≤gcd
    - True unless [a mod min] or [b mod min] non-zero
    - Assume wlog a = k·min + t for 0<t<min
    - Then t = a - k·min = a-k(ra+sb) = (1-kr)a-(ks)b
    - But then by definition min ≤ t giving a contradiction

- Theorem:
  If $c|ab$ and $\gcd(a,c)=1$ then $c|b$
- Proof:
  - Since $\gcd(a,c)=1$ there are r,s such that
    $1 = ra+sc$
  - Multiply by b to get
    $b = rab+scb$
  - This gives
    $b = (r(ab/c) + sb)c$
  - So $c|b$

- Theorem:
  If $a|N$ and $b|N$ and $gcd(a,b)=1$ then $ab|N$

- Proof:
  - Since $a|N$ we can write $N=ra$
  - Since $b|ra$ and $gcd(a,b)=1$ we get from the previous theorem $b|r$
  - Write $r=sb$ and we now have $N=sba$

- End of material covered on September 30 -

Euclidean algorithm

- Theorem:
  If a|b then gcd(a,b) = a
  else gcd(a,b) = gcd(a, b mod a)
- Proof:
  - Suppose d|a and d|b, then d|a and d|b-xa
  - Suppose d|a and d|b-xa, then d|a and d|b
  - Can compute gcd(a,b) with b>a as follows:

    gcd(a,b) = gcd(a,c) where c = b mod a

    gcd(a,c) = gcd(d,c) where d = a mod c

    …

Extended Euclidian example

- gcd(13,18) = 1   so $1 = x\cdot 13 + y\cdot 18$
  - Write z = (a,b) for z = a13+b18
  - 18 = (0,1)   and 13 = (1,0)
  - 18 mod 13
    = 5 = 18 – 13 = (0,1) – (1,0) = (-1,1)
  - 13 mod 5
    = 3 = 13 – 2·5 = (1,0) – 2(-1,1) = (3,-2)
  - 5 mod 3
    = 2 = 5 – 3 = (-1,1) – (3,-2) = (-4,3)
  - 3 mod 2
    = 1 = 3 – 2 = (3,-2) – (-4,3) = (7,-5)
- So $1 = 7\cdot 13 - 5\cdot 18$

Modular arithmetic

- Many of the usual laws of the integers apply also when computing modulo N
- Associativity:
- $(a+b \bmod N)+c \bmod N$
  $= a+(b+c \bmod N) \bmod N$
  $= a+b+c \bmod N$
- $(ab \bmod N)c \bmod N$
  $= a(bc \bmod N) \bmod N$
  $= abc \bmod N$

Commutative ring Z_N

- $(a+b)+c = a+(b+c) \bmod N$
- $a+0 = 0+a = a \bmod N$
- $a+(-a) = (-a)+a = 0 \bmod N$
- $a+b = b+a \bmod N$
- $(ab)c = a(bc) \bmod N$
- $1a=a1=a \bmod N$
- $ab = ba \bmod N$
- $a(b+c) = ab+ac \bmod N$
- $(a+b)c = ac+bc \bmod N$

Multiplicative inverses?

- Some numbers have inverses
  - Take 3 mod 10
  - $3 \bullet 7 = 21 = 1 + 20 = 1 \bmod 10$
  - So 3 has an inverse
- But not all numbers have inverses
  - Look at 2 mod 10
  - There is no number b so $2b = 1 \bmod 10$
- We define $\mathbf{Z}_N{}^*$ = invertible elements in $\mathbf{Z}_N$

Multiplicative inverses

- Element a has multiplicative inverse modulo N if and only if gcd(a,N) = 1
- Proof:
  - If gcd(a,N) = 1 we can write ra+sN=1 so ra = 1 mod N, i.e., r is an inverse to a
  - If on the other hand a has an inverse r, then ra=1 mod N, which means ra+sN=1 and therefore gcd(a,N)=1
- We write a^{-1} for the inverse of a
- The inverse is unique modulo N

Exercise

- What is $\mathbf{Z}_{12}$?
- What is $\mathbf{Z}_{12}^*$?
- For each element in $\mathbf{Z}_{12}^*$, find its inverse
- Answers:
  - $\mathbf{Z}_{12} = \{0,1,2,3,\ldots,11\}$
  - $\mathbf{Z}_{12}^*=\{1,5,7,11\}$ (gcd(a,12)=1)
  - Inverses: 1,5,7,11
- Trick:
  - 11 = -1 mod 12, 7 = -5 mod 12

Exercise II

- What is $\mathbf{Z}_{23}$?
- What is $\mathbf{Z}_{23}$*?
- For each element in $\mathbf{Z}_{23}$* find its inverse
- Answers:
  - $\mathbf{Z}_{23} = \{0,1,2,3,\ldots,22\}$
  - $\mathbf{Z}_{23}^* = \{1,2,3,4,\ldots,22\}$ (gcd(a,23)=1)
  - Element:1, 2, 3,4, 5,6, 7,8, 9,10,11,-11,-10,…
  - Inverse: 1,12,8,6,-9,4,10,3,-5, 7,-5, 5, -7,…

The finite field $\mathbf{Z}_p$

- What is $\mathbf{Z}_p$* when p is a prime?
- The elements that have gcd(a,p)=1
- We have gcd(a,p) = 1 for all a not divisible by p
- So $\mathbf{Z}_p^* = \{1,2,3,\ldots,p-1\}$
- A field is a commutative ring where all non-zero elements are invertible
- $\mathbf{Z}_p$ is a field with p elements

Group

- A group G is a set of elements with a binary operation • : $G \times G \rightarrow G$ obeying the following laws:
- Associativity: $(a \bullet b) \bullet c = a \bullet (b \bullet c)$
- Neutral element: $e \bullet a = a \bullet e = a$
- Inverse: $a \bullet a^{-1} = a^{-1} \bullet a = e$
- The group is said to be abelian if it is Commutative: $a \bullet b = b \bullet a$

Example

- $\mathbf{Z}_N$ = {0,1,…,N-1} is a finite abelian group
- The binary operation is addition mod N
- Associative: $(a+b)+c = a+(b+c) \bmod N$
- Neutral element: $0+a=a+0=a \bmod N$
- Inverse: $a+(-a) = (-a)+a = 0 \bmod N$
- Commutative: $a+b = b+a \bmod N$

Example

- $\mathbf{Z}_N$* is a finite abelian group
- Binary operation is multiplication modulo N
- Associative: $(ab)c = a(bc) \bmod N$
- Neutral element: $1a = a1 = a \bmod N$
- Inverse: $aa^{-1} = a^{-1}a = 1 \bmod N$
- Commutative: $ab = ba \bmod N$

Subgroups

- H is called a subgroup of G, and we write H≤G, if H is a subset of G and is a group with the same binary operation
- Example: $\{0,2,4,6\} \leq \mathbf{Z}_8$
- Example: $\{1,4\} \leq \mathbf{Z}_5{}^*$
- Lagrange's theorem:
  If H≤G then |H| divides |G|

Lagrange's Theorem

Theorem:

If $H \leq G$ then $|H|$ divides $|G|$

Proof:

- For all g: $|H|=|gH|$
  - Bijection: $h \leftrightarrow gh$
- For all g,g': $gH=g'H$ or $gH \cap g'H=\emptyset$
  - If $gh=g'h'$ then $g=g'h'h^{-1}$ so $gH=g'h'h^{-1}H=g'H$
- Write $G = g_1H \cup \ldots \cup g_kH$ with disjoint sets to see $|G|=k|H|$

Cyclic groups

- Definition:
  $g^i = g \bullet g \bullet ... \bullet g$ (i times)
  $g^0=1$ and $g^{-i}=(g^{-1})^i$
- Theorem: $H=\{\ldots g^{-2},g^{-1},1,g,g^2,\ldots\}$ is an abelian subgroup of G
- Proof:
  - Closure: $g^i g^j=g^{i+j}$
  - Associativity: $(g^i g^j)g^k=g^{i+j+k}=g^i(g^j g^k)$
  - Neutral element: $1g=g1=g$
  - Inverses: $g^i g^{-i}=g^{-i}g^i=1$
  - Commutativity: $g^i g^j=g^{i+j}=g^j g^i$

Order of finite group

- Definition:
  The order of a group is the number of elements, i.e., $ord(G)=|G|$
- Theorem: For all $g \in G$ we have $g^{|G|} = 1$
- Proof:
  - Let $H = \{\ldots g^{-2}, g^{-1}, 1, g, g^2, \ldots\}$ and let k be the smallest k so $g^i=g^{i+k}$ for some i.
  - Then $g^k=1$ and hence $H = \{1, g, \ldots, g^{k-1}\}$.
  - Since it is a subgroup of G we have $k|ord(G)$ so $g^{|G|}=1$

Examples

- Examples:
  - In $\mathbf{Z}_6$ we have $|\mathbf{Z}_6|=6$ and for g=2
    $2+2+2+2+2+2 = 2\cdot 6 = 0 \bmod 6$
  - In $\mathbf{Z}_7^*$ we have $|\mathbf{Z}_7^*|=6$ and for g=2 that
    $2\cdot 2\cdot 2\cdot 2\cdot 2\cdot 2 = 2^6 = 64 = 1 \bmod 7$
- Fermat's Little Theorem:
  If p prime then $g^p - g = 0 \bmod p$
- Proof:
  - Clear if $g=0 \bmod p$
  - And else $g^{p-1}=1 \bmod p$ (previous theorem)

Finite cyclic groups

- A finite group G is cyclic if there is an element g such that $G = \{1, g, g^2, \ldots\}$
- We say g is a generator of G and write G = <g>
- $\mathbf{Z}_{12}$ is cyclic with generator 1, i.e., we can write all $x = 1+1+\ldots+1 = 1 \cdot x \bmod 12$
- $\mathbf{Z}_5^* = \{1, 2, 2^2, 2^3\}$ (all mod 5) is cyclic
- Theorem (without proof):
  If p is prime then $\mathbf{Z}_p^*$ is cyclic

Exercise II from earlier

- Is $\mathbf{Z}_{23}^* = \{1,2,\ldots,22\}$ cyclic?
- Yes, p=23 is a prime, so it is cyclic
  - There is a generator g such that $\mathbf{Z}_{23}^*=\langle g \rangle$
- Is g = 2 a generator?
  - No, g=2 gives $\langle 2 \rangle=\{2,4,8,16,9,18,13,3,6,12,1\}$
- Is g = 20 a generator?
  - Simplification: 20 = -3 mod 23
  - Yes, g=-3 gives us (modulo 23)
    $(-3)^1=-3$, $(-3)^2=9$, $(-3)^3=-4$, $(-3)^4=11$, $(-3)^5=-10$, $(-3)^6= 7$, $(-3)^7=-2$, $(-3)^8=6$, $(-3)^9= 5$, $(-3)^{10}=8$, $(-3)11=-1$, ... , $(-3)^{22}=12$

Simpler method

- $\mathbf{Z}_{23}^* = \{1,2,\ldots,22\}$ is a cyclic group
- Is g = -3 a generator?
  - Yes, g=-3 gives us (modulo 23)
    $(-3)^1=-3$, $(-3)^2=9$, $(-3)^3=-4$, $(-3)^4=11$, $(-3)^5=-10$, $(-3)^6= 7$, $(-3)^7=-2$, $(-3)^8=6$, $(-3)^9= 5$, $(-3)^{10}=8$, (-3)11=-1, ... , $(-3)^{22}=1$
- Observe, <-3> is a subgroup of $\mathbf{Z}_{23}^*$
- This means $|\langle -3\rangle|$ divides $|\mathbf{Z}_{23}^*|=22$
- Four options: $|\langle -3\rangle| \in \{1,2,11,22\}$
- If $(-3)^1\neq 1,(-3)^2\neq 1,(-3)^{11}\neq 1$ then $|\langle -3\rangle|=|\mathbf{Z}_{23}^*|$

Probability - Further reading

- KL: Appendix A
- Trevisan’s Discrete Prob. (first 7 pages)
  - See Moodle, optional

Algebra & Number Theory

- Further reading:
  - Tsudik’s algebra review (slides)
  - Boneh’s intro to number theory (slides)
  - KL Appendix B, 7.1, 7.2
- More:
  - Shoup’s intro to number theory and algebra
  - Stallings 8.1, 8.2, 8.3, 8.4