MATH 314 Fall 2019 - Class Notes

9/16/2019

Scribe: Jay Romero

Summary : Classical Ciphers and Elementary Number Theory

Notes:

One-Time Pads

- It is a Vigenere cipher where key has the same length as the plaintext.
- Key is a completely random string of letters.
- Can only use a key one-time hence the name.
- It is a mathematically unbreakable cipher.
- DOWNSIDE: You need to use a new key for every message sent and key size is as big as the message being sent which is not practical.

Elementary Number Theory

Find $\gcd(a, b)$

- One idea is to use trial division where you try dividing both a, b by all the numbers up to $\min{(a,b)} take the largest number that divides both.$
  How long will this approach take? $n = \min{(a,b)}$
  Let x = number of bits required to write n in base 2

$$x = \lceil \log_2 n \rceil$$

If we do n-trial divisions then running time $O(n)$ =O(2^x)

- Another approach is the factorization method, that is, factor a, b into primes, find gcd by taking all primes that divide both.
- The fastest known algorithm for factoring an x-bit number runs in $O(e\sqrt{}$x $\ln{(x)})$ Sub-exponential but still much slower than polynomial time.
- The best approach is Euclids Algorithm where reunning time is $O(x)$ =O($\log n$)
- Key idea: Division with remainder

- Fact: Given any two positive integers a, b there exist two integers q, r with $a = bq + r$ and $0 \leq r < b$.

  Proof.

  Given a, b compute $q \equiv \lfloor \frac{a}{b} \rfloor$ then compute $r = a - bq$
  NOTE: $r + bq = a$
  Need to show that $0 \leq r < b$

  $$\frac{a}{b} - 1 < \lfloor \frac{a}{b} \rfloor \leq \frac{a}{b} \Rightarrow \frac{a}{b} - 1 < q \leq \frac{a}{b}$$

  Now multiply through by b yields

  $$a - b < qb \leq a$$

  Soqb $\leq a \Rightarrow 0 \leq a - qb = r$ so $0 \leq r$
  $a - b < qb$
  $r = q - qb < b \Rightarrow r < b >$ □

- If d divides n and m then d divides n + m and n - m

Suppose $d = \gcd(a, b)$
Write $a = bq + r$
$r = a - bq$
d has to divide r so $\gcd(a, b) = \gcd(b, r)$
Apply this recursively. Repeat until we get a remainder of 0. The answer is the previous remainder.
Example: $\gcd(158, 38)$
Use division with remainder

$$158 = 4(38) + 6$$

$$So\, \gcd(158, 38) = \gcd(38, 6)$$

$$38 = 6(6) + 2 \Rightarrow \gcd(158, 38) = \gcd(38, 6) = \gcd(6, 2)$$

$$6 = 3(2) + 0$$

$$So\, \gcd(158, 38) = 2$$

Extended Euclidian Algorithm
If $gcd(a, b) = d$ then there exist integers x and y so that $ax + by = d$
Euclid Algorithm tells us how to find x and y

Use Euclids Algorithm backward. Start with the equation that gave last remainder and solve it for d.

$$2 = 38 - 6(6)$$

Solve the next equation for its remainder.
Substitute in.

$$6 = 158 - 4(38)$$
$$\Rightarrow 2 = 38 - 6(158 - 4(38)) \Rightarrow 2 = -6(158) + 25(38)$$

Example: Find x and y so that $72x + 25y = 1$

Use Euclidean Algorithm forward $\gcd(72, 25)$

$$\begin{aligned} 72 &= 2(25) + 22 \\ 25 &= 1(22) + 3 \\ 22 &= 7(3) + 1 \\ 3 &= 3(1) + 0 \end{aligned}$$

So GCD = 1

Now use Euclidean Algorithm backwards

$$1 = 22 - 7(3)$$
$$3 = 25 - 1(22)$$
$$So1 = 22 - 7(25 - 1(22))$$
$$= -7(25) + 8(22)$$

Since

$$22 = 72 - 2(25)$$

Substitute gives us

$$1 = -7(25) + 8(72 - 2(25)) \Rightarrow 1 = 8(72) - 23(25)$$

where $x = 8$ and $y = -23$