Week 5: Applications to Cryptograph and Proofs by Induction

Agenda:

- More example of proof techniques
- Operations mod n and an application
- Induction

Reading:

- Textbook pages 179–227.

- **Theorem:** $\sqrt{2}$ is irrational.

  Proof: By way of contradiction, assume that $\sqrt{2}$ is rational, i.e. there are integers $a, b \neq 0$ such that $\sqrt{2} = \frac{a}{b}$.

  Without loss of genrality, we assume that a and b do not have any commont factors other than 1 (i.e. are relatively prime to each other) otherwise, we can cancel out any common factors they have. Then:

  $$2 = \frac{a^2}{b^2} \qquad \Longrightarrow \quad 2b^2 = a^2.$$

  Since a^2 is even (the LHS is even because has a factor of 2), so must be a; that is $a = 2k$ for some integer k. Thus:

  $$2b^2 = (2k)^2 = 4k^2 \quad \Longrightarrow \quad b^2 = 2k^2.$$

  This implies that b^2 is even which in turn means b must be even. But then both a and b have a common factor (of 2, as they are even); which contradicts our assumption.

Arithmetic Operations in mod n

- (m mod n) is the reminder of dividing m by n; i.e. if $m = nq + r$ for some $0 \leq r < q$, then m mod $n = r$

  e.g. 21 mod $9 = 3$ and 15 mod $4 = 3$

- **Theorem:** i mod $n = (i + kn)$ mod n, for any integer k.

  Proof: By Quotient Reminder Theorem, there are unique integers q and $0 \leq r < q$ such that $i = nq + r$. So $i + kn = nq + r + kn = n(q + k) + r$ which implies $i + kn$ mod $n = r$.

- **Theorem:** $(i + j)$ mod $n = ((i$ mod $n) + (j$ mod $n))$ mod n and (ij) mod $n = ((i$ mod $n)(j$ mod $n))$ mod n.

  Proof: We prove the first statement. The proof of the second one is almost identical. By Q-R Theorem, there are unique integers q_1

and q_2 such that $i = q_1 n + (i \bmod n)$ and $j = q_2 n + (j \bmod n)$. Therefore:

$$\begin{aligned}
(i+j) \bmod n &= (q_1 n + (i \bmod n) + q_2 n + (j \bmod n)) \bmod n \\
&= ((q_1 + q_2)n + (i \bmod n) + (j \bmod n)) \bmod n \\
&= ((i \bmod n) + (j \bmod n)) \bmod n
\end{aligned}$$

where the last equality uses the previous theorem.

- Using this theorem, it is easy to prove the following:

  Theorem: $a^{i+j} \bmod n = ((a^i \bmod n)(a^j \bmod n)) \bmod n$.

- Some examples:

  $3^0 \bmod 7 = 1$
  $3^1 \bmod 7 = 3$
  $3^2 \bmod 7 = (3 \bmod 7)^2 \bmod 7 = 2$
  $3^3 \bmod 7 = ((3^2 \bmod 7)(3 \bmod 7)) \bmod 7 = 6$
  $3^4 \bmod 7 = ((3^3 \bmod 7)(3 \bmod 7)) \bmod 7 = 4$
  $3^5 \bmod 7 = 5$
  $3^6 \bmod 7 = 1$
  $3^7 \bmod 7 = 3$

A puzzle with application in Cryptography

- There are two people Alice and Bob that want to agree on some secrete key.

- There is a communication line they can use which is not secure; a malicious third party, Eve, is tapping the line.

- Eve can see everything being transmitted on the line (but cannot change it).

- How can Alice and Bob do this seemingly impossible task?

- Solution: First Alice and Bob agree on some prime number p with a few hundred bits and some other integer $2 \leq g \leq p-1$ (one of them picks the numbers and sends to the other).

- It is Ok if Eve sees p and g.

- Alice and Bob choose random numbers A and B respectively each from $2, \ldots, p-1$.

- Then Alice computes $a = g^A \ \ mod\, p$ and sends to Bob

  Bob comptues $b = g^B \ \ mod\, p$ and sends to Alice

- Now Alice computes $x = b^A \ \ mod\, p$ and

  Bob computes $y = a^B \ \ mod\, p$.

- Note that $x = g^{AB} \ \ mod\, p$ and $y = g^{BA} \ \ mod\, p \Longrightarrow$ $x = y$; now x is their secret common key.

- The only operations that Alice and Bob do are exponentiation and mod.

- What can Eve do to find out the key x? She has values of p, g, a, and b

- So Eve needs to compute an integer A' s.t. $a = g^{A'} \ \ mod\, p$ and then calculate $x' = b^{A'} \ mod\, p$.

- If p is an odd prime then A' must be equal to A and so $x' = x$.

- For this, Eve needs compute the discrete logarithm of a in base g; but all known algorithms for computing discrete logarithm of a number a take about $\sim a$ steps.

- note that a is a number with hundreds of bits (say 400 bits); so the value of a is in the range of 2^{400}; it takes Eve forever to compute the discrete log then.

- What about Alice and Bob? how easy/fast is to compute the exponentiation and mod?

- The naive algorithm to compute g^A takes g and multiplies it $A-1$ times; so takes roughly A multiplications.

- If A has a few hundred bits (say 400) this is going to take $\approx 2^{400}$ steps for Alice and Bob too!!

- So not only Eve cannot find the secret, even Alice and Bob cannot compute their secret either.

- But there is a faster way to compute g^A;

- Observation:
$$g^{24} = (g^{12})^2 = ((g^6)^2)^2 = (((g^3)^2)^2)^2 = (((((g^2 \cdot g)^2)^2)^2$$

- note that taking square of a number needs only one multiplication; this way, to compute g^{24} we need only 5 multiplication instead of 24.

- In general, using this technique, it will require about $\sim 2 \log A$ multiplications to compute g^A. If A has 400 bits, then $\log A$ is about 400, and so Alice and Bob only need to do about 800 multiplications.

Inductive proofs

- *Squence:* A (possibly infinite) row of numbers. e.g. $1, 4, 9, 16, 25, \ldots$. We may rewrite this as $a_1, a_2, \ldots,$ where $a_i = i^2$ for $i \geq 1$.

- A sequence could be finite/infinite

- The number of distinct values could be finite/infinite

- There could be multiple explicit/general formulae

Summations and Products:

- $$\sum_{k=m}^{n} a_k = a_m + a_{m+1} + \ldots + a_n$$

  E.g., $\displaystyle\sum_{k=1}^{4} k^2 = 1^2 + 2^2 + 3^2 + 4^2 = 30$

- Note: $n \geq m$, otherwise there is no term in the summation

- $$\prod_{k=m}^{n} a_k = a_m \cdot a_{m+1} \cdot \ldots \cdot a_n$$

- n factorial (n positive integer) is $n! = \displaystyle\prod_{k=1}^{n} k$

  $0! = 1$

Properties:

- $$\sum_{k=m}^{n} a_k + \sum_{k=m}^{n} b_k = \sum_{k=m}^{n} (a_k + b_k)$$

- c $\displaystyle\sum_{k=m}^{n} a_k = \sum_{k=m}^{n} ca_k$

- $\displaystyle\left(\prod_{k=m}^{n} a_k\right) \cdot \left(\prod_{k=m}^{n} b_k\right) = \prod_{k=m}^{n} (a_k \cdot b_k)$

Mathematical Induction:

- **Principle (axiom)**: Let $P(n)$ be a property defined for integers n, and a a fixed integer
  - $P(a)$ is true
  - For all integers $k \geq a$, if $P(k)$ is true then $P(k+1)$ is true

  Then, "for all integers $n \geq a$, $P(n)$" is true.

- Proof by (the principle of) Mathematical Induction:
  - (basis step): $P(a)$ is true
  - (inductive step): Show that for all integers $k \geq a$, if $P(k)$ is true then $P(k+1)$ is true

- Example: Prove that for all $n \geq 1$: $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$.

  Proof: Let predicate $P(n)$ be "$\sum_{i=1}^{n} i = n(n+1)/2$". We prove that $P(n)$ holds for all values of $n \geq 1$ by induction.

  Basis: For $n = 1$ we have $\sum_{i=1}^{1} = 1 = 1(1+1)/2$; so $P(1)$ holds.

  Ind. Step: Let $k \geq 1$ be an arbitrary integer and assume that $P(k)$ holds. We prove that $P(k+1)$ holds.

$$\begin{aligned}
\sum_{i=1}^{k+1} i &= \sum_{i=1}^{k} +(k+1) \\
&= \frac{k(k+1)}{2} + (k+1) \quad \text{by induction hyp that } P(k) \text{ holds}
\end{aligned}$$

$$
\begin{aligned}
&= \frac{k(k+1)}{2} + \frac{2(k+1)}{2} \\
&= \frac{(k+1)(k+2)}{2}
\end{aligned}
$$

as wanted. So $P(k+1)$ holds.

- Example: Prove that for every real $r \neq 1$ and every integer $n \geq 0$: $\sum_{i=0}^{n} r^i = \frac{r^{n+1}-1}{r-1}$.

  Proof: Let $P(n)$ be "for every real $r \neq 1$, $\sum_{i=0}^{n} r^i = \frac{r^{n+1}-1}{r-1}$". We prove $P(n)$ holds for all integers $n \geq 0$.

  Basis: For $n = 0$: $\sum_{i=0}^{0} r^i = 1 = \frac{r-1}{r-1}$, so $P(0)$ holds.

  Ind. Step: Let $k \geq 0$ be an arbitrary integer and assume that $P(k)$ holds. We prove $P(k+1)$.

$$
\begin{aligned}
\sum_{i=0}^{k+1} r^i &= \left(\sum_{i=0}^{k} r^i\right) + r^{k+1} \\
&= \frac{r^{k+1}-1}{r-1} + r^{k+1} \quad \text{by ind. hyp} \\
&= \frac{r^{k+1}-1+r^{k+1}(r-1)}{r-1} \\
&= \frac{r^{k+2}-1}{r-1},
\end{aligned}
$$

  So $P(k+1)$ holds.

- Example: Any amount of postage greater than or equal to $8c$ can be paid for using only $5c$ and $3c$ stamps.

  Proof: Let $P(n)$ be "n cent postage can be paid for using $5c$ and $3c$ stamps".

  We prove $P(n)$ holds for all $n \geq 8$.

  Basis: Clearly $P(8)$ is true as you pay by one $5c$ and one $3c$ stamp.

Ind. Step: Let $k \geq 8$ be an arbitrary integer and assume that $P(k)$ is true; i.e. there are integers $x, y \geq 0$ s.t. $k = 3x + 5y$ (x being the number of 3c stamps and y being the number of 5c stamps.

We prove that $P(k+1)$ is true. Consider two cases:

- Case 1: if $y \geq 1$ then we can replace a 5c stamp with two 3c stamps: so $k + 1 = 3(x + 2) + 5(y - 1)$.
- Case 2: if $y = 0$ then because $k \geq 8$ we must have at least three 3c stamps, i.e. $x \geq 3$. So we can replace three 3c stamps with two 5c stamps and get: $k + 1 = 3(x - 3) + 5(y + 2)$;

In either case we can pay for $k + 1$ cents; thus $P(k + 1)$ holds.

- Example: Prove that for every real x s.t. $1 + x > 0$ and all integers $n \geq 0$: $(1 + x)^n \geq 1 + nx$.

  Let $P(n)$ be the predicate: "with $1 + x > 0$ we have $(1 + x)^n \geq 1 + nx$".

  We prove $P(n)$ for all values of $n \geq 0$.

  Basis: For $n = 0$: $(1 + x)^0 = 1 \geq 1 + 0.x$; so $P(0)$ holds.

  Ind. Step: Let $k \geq 0$ be an arbitrary integer and assume that $P(k)$ holds.

  We prove that $P(k + 1)$ holds too.

$$
\begin{aligned}
(1+x)^{k+1} &= (1+x)^k(1+x) \\
&\geq (1+kx)(1+x) \qquad \text{by } P(k) \text{ and because } 1+x>0 \\
&= 1 + x + kx + kx^2 \\
&\geq 1 + (k+1)x \quad \text{because } kx^2 \geq 0 \text{ always}
\end{aligned}
$$