Lecture 12.

It’s Friday.
Will let out early today!
61A midterm makeup afterwards.

Today: A bit of review, RSA, signature schemes.

---

Excursion: Bijections.

\[ f : S \to T \text{ is one-to-one mapping.} \]
\[ \text{one-to-one: } f(x) \neq f(x') \text{ for } x, x' \in S \text{ and } x \neq x'. \text{ Not 2 to 1!} \]
\[ f() \text{ is onto.} \]
\[ \text{If for every } y \in T \text{ there is } x \in S \text{ where } y = f(x). \]

Bijection is one-to-one and onto function.
Two sets have the same size
if and only if there is a bijection between them!

**Same size?**
- \{red, yellow, blue\} and \{1, 2, 3\}?
  - \(f(\text{red}) = 1, f(\text{yellow}) = 2, f(\text{blue}) = 3\).
  - \(\text{red, yellow, blue}\) and \{1, 2, 3\}?
  - \(f(\text{red}) = 1, f(\text{yellow}) = 2, f(\text{blue}) = 2\).

\[ \text{two to one! not one to one.} \]
- \{red, yellow\} and \{1, 2, 3\}?
  - \(f(\text{red}) = 1, f(\text{yellow}) = 2\).

\[ \text{Misses 3, not onto.} \]

---

Inverses?

When does \(a\) have inverse \((\text{mod } m)\)?

When \(\gcd(a, m) = 1!\)

---

Proof review.

**Claim:** \(a^{-1} \pmod{m}\) exists when \(\gcd(a, m) = 1!\)

**Fact:** \(ax \neq ay \pmod{m}\) for \(x \neq y \in \{0, \ldots, m-1\}\)

**Proof of Fact:** Let \(ax = ay \pmod{m}\), \(x \neq y \in \{0, \ldots, m-1\}\)
\[ ax = ay + km \]

Consider prime factorization:
\[ a = a_1 \cdots a_k \]
\[ m = m_1 \cdots m_l \]

Do any \(a_i = m_j\)? Yes? No? No! \(\gcd(a, m) = 1!\)

Therefore \(a(x - y) = km\)

only if factorization of \((x - y)\) contains all factors of \(m\).

\[ \implies (x - y) \geq m \text{ or } (x - y) = 0. \]

Contradiction.

---

Modular arithmetic examples.

\[ f : S \to T \text{ is one-to-one mapping.} \]
\[ \text{one-to-one: } f(x) \neq f(x') \text{ for } x, x' \in S \text{ and } x \neq y. \]
\[ f() \text{ is onto.} \]
\[ \text{If for every } y \in T \text{ there is } x \in S \text{ where } y = f(x). \]

Recall:
\[ f(\text{red}) = 1, f(\text{yellow}) = 2, f(\text{blue}) = 3 \]

One-to-one if inverse:
\[ g(1) = \text{red}, g(2) = \text{yellow}, g(3) = \text{blue}. \]

Is \(f(x) = x + 1 \pmod{m}\) one-to-one?
\[ g(x) = x - 1 \pmod{m}. \]

Onto: range is subset of domain.

Is \(f(x) = ax \pmod{m}\) one-to-one?

If \(\gcd(a, m) = 1, ax \neq ax' \pmod{m}. \)

Injective? Surjective?
We tend to use one-to-one and onto function.

**Bijection** is one-to-one and onto function.
Two sets have the same size
if and only if there is a bijection between them!

---

Inverses: continued.

**Claim:** \(a^{-1} \pmod{m}\) exists when \(\gcd(a, m) = 1!\)

**Fact:** \(ax \neq ay \pmod{m}\) for \(x \neq y \in \{0, \ldots, m-1\}\)

Consider \(T = \{0a \pmod{m}, 1a \pmod{m}, \ldots, (m-1)a \pmod{m}\}\)

Consider \(S = \{0, 1, \ldots, (m-1)\}\)

\(S = T. \) Why?

\(T \subseteq S\) since \(ax \pmod{m} \in \{0, \ldots, m-1\}\)

One-to-one mapping from \(S\) to \(T\)!

\[ \implies |T| \geq |S| \]

Same set.

Why does a have inverse? \(T\) is \(S\) and therefore contains 1 ! ! !

Why am I excited? There is an \(x\) where \(ax = 1. \)
There is an inverse of \(a!\) ! !
Fermat from Bijection.

Fermat’s Little Theorem: For prime \( p \) and any \( a \neq 0 \pmod{p} \),
\[ a^{p-1} \equiv 1 \pmod{p}. \]

Proof: Consider \( T = \{a \cdot 1 \pmod{p}, \ldots a \cdot (p-1) \pmod{p}\} \).
\( T \) is range of function \( f(x) = ax \mod{p} \) for set \( S = \{1, \ldots, p-1\} \).
Invertible function: one-to-one.
\( T \subset S \) since \( 0 \not\in T \).
\( p \) is prime.

\[ \Rightarrow T = S. \]
Product of elts of \( T \) = Product of elts of \( S \).
\( (a \cdot 1) \cdot (a \cdot 2) \cdot (a \cdot (p-1)) = 1 \cdot 2 \cdot (p-1) \pmod{p}, \)
Since multiplication is commutative.
\[ a^{p-1} \equiv 1 \pmod{p}. \]
Each of \( 2 \ldots (p-1) \) has an inverse modulo \( p \), multiply by inverses to get...
\[ a^{p-1} \equiv 1 \pmod{p}. \]

Lemma 1: For any prime \( p \) and any \( a, b \),
\[ a^{1+k(p-1)} \equiv a \pmod{p}. \]

Lemma 2: For any two different primes \( p, q \) and any \( x, k \),
\[ x^{1+k(q-1)(p-1)} \equiv x \pmod{pq}. \]

Let \( a = x, b = k(p-1) \) and apply Lemma 1 with modulus \( q \).
\[ x^{1+k(q-1)(p-1)} \equiv x \pmod{q}. \]
\[ x^{1+k(q-1)(p-1)} - x \equiv 0 \pmod{q} \Rightarrow \text{multiplie of } q. \]
Let \( a = x, b = k(q-1) \) and apply Lemma 1 with modulus \( p \).
\[ x^{1+k(q-1)(p-1)} \equiv x \pmod{p}. \]
\[ x^{1+k(q-1)(p-1)} - x \equiv 0 \pmod{p} \Rightarrow \text{multiplie of } p. \]
\[ x^{1+k(q-1)(p-1)} - x \equiv 0 \pmod{pq} \Rightarrow x^{1+k(q-1)(p-1)} \equiv x \pmod{pq}. \]

RSA and Fermat.

RSA:

Alice:

- Primes: \( p, q \), \( N = pq \).
- Encryption Key: \( e \) where \( gcd(e,(p-1)(q-1)) = 1 \).
- Decryption Key: \( d = e^{-1} \pmod{(p-1)(q-1)} \).
- Message: \( m \).
- Encryption: \( y = E(m) = m^e \pmod{N} \).
- Decryption: \( D(y) = y^d \pmod{N} \).

Result: \( m^{ed} \equiv m \pmod{N} \).

Example:
\( p = 7, q = 11, N = 77 \)
\( x = 2 \)
\( y = 2^7 \pmod{77} \).
\( x^d = 2 \pmod{77} \).

Alice got Bob’s message!

Idea: Fermat removes the \( k(p-1) \) from the exponent!

Lemma 2: For any two different primes \( p, q \) and any \( x, k \),
\[ x^{1+k(p-1)(q-1)} \equiv x \pmod{pq}. \]

Theorem: RSA correctly decodes!

Recall
\[ D(E(x)) = (x^e)^d = x^{ed} \equiv x \pmod{pq}, \]
where \( ed = 1 \pmod{(p-1)(q-1)} \).
\[ x^{ed} = x^{k(p-1)(q-1)+1} = x \pmod{pq}. \]

RSA decodes correctly.

Fermat: a seeming excursion?

Thm: \( m^{ed} \equiv m \pmod{pq} \) if \( ed = 1 \pmod{(p-1)(q-1)} \).

Seems like magic!

Fermat’s Little Theorem: For prime \( p \) and \( a \neq 0 \pmod{p} \),
\[ a^{p-1} \equiv 1 \pmod{p}. \]

Thm: \( 3^6 \pmod{7} = 1 \).
\( 3^2 \pmod{7} = 3 \).

Involves exponents and gets 3 back.
Seems like magic.

Corollary: \( a^{k(p-1)+1} = a \pmod{p} \).

Get a back when exponent is 1 \pmod{p-1}.
A little like RSA.
Seems like magic!

Proof of Corollary: If \( a = 0 \), \( a^{k(p-1)+1} = 0 \pmod{m} \).
Otherwise \( a^{k(p-1)+1} = a \cdot (a^{k(p-1)})^k = a \cdot (1)^k = a \pmod{p} \).

Idea: Fermat removes the \( k(p-1) \) from the exponent!

Construction of keys...

1. Find large (100 digit) primes \( p \) and \( q \).
2. Choose \( e \) with \( gcd(e,(p-1)(q-1)) = 1 \).
3. Find inverse \( d \) of \( e \) modulo \( (p-1)(q-1) \).

Prime Number Theorem: \( \pi(N) \) number of primes less than \( N \).
For all \( N \geq 17 \),
\[ \pi(N) \geq N / \ln(N). \]
Choosing randomly gives approximately \( 1/(\ln N) \) chance of number being a prime. (How do you tell if it is prime? ...)

All steps are polynomial in \( O(\log N) \), the number of bits.
Security of RSA.

1. Alice knows $p$ and $q$.
2. Bob only knows $N (= pq)$, and $e$. Does not know, for example, $d$ or factorization of $N$.
3. Breaking this scheme $\Rightarrow$ factoring $N$. Don't know how to factor $N$.

Much more to it.....

If Bobs sends a message (Credit Card Number) to Alice, Eve sees it. Eve can send credit card again!!

The protocols are built on RSA but more complicated; For example, several rounds of challenge/response.

One trick:
Bob encodes credit card number, $c$, concatenated with random $k$-bit number $r$.
Never sends just $c$.
Again, more work to do to get entire system.
CS161...