Recitation 4: Number theory review and practice problems

6.5610, Spring 2023

March 3, 2023

1 Number theory

1.1 Basic stuff

- We'll be going over some number theory, specifically related to groups with modulus. These groups have some (believed to be) hard problems and some easy problems that are useful in Diffie-Hellman key exchange, ElGamal encryption, RSA encryption, and more.
- For a prime p, let $Z_p = \{0, 1, 2, \ldots, p-1\}$. We can add and multiply elements modulo p.
- Fermat's theorem says that for any $x \in Z_p^*$ we have: $x^{p-1} = 1 \mod p$.

  Example: for $p = 5$, $3^4 = 81 = 1 \mod 5$
- The inverse of $x \in Z_p$ is an element a such that $a \cdot x = 1 \mod p$. The inverse of x modulo p is denoted by x^{-1}.

  Example: $3^{-1} \mod 5 = 2$ since $2 \cdot 3 = 6 = 1 \mod 5$
- $Z_p^* = \{1, 2, \ldots, p-1\}$, the set of invertible elements in Z_p.

1.2 Structure of Z_p^*

- Z_p^* is a cyclic group. In other words, there exists a generator g such that $Z_p^* = \{1, g, g^2, \ldots, g^{p-2}\}$.

  Example: in Z_7^*, 3 is a generator because $\{1, 3, 3^2, \ldots, 3^5\} = \{1, 3, 2, 6, 4, 5\} \mod 7 = Z_7^*$
- Not every element of Z_p^* is a generator.

  Example: 2 is not a generator for Z_7^* because $\{1, 2, 2^2, 2^3\} = \{1, 2, 4, 1\} \mod 7$, and this cycle will loop and it will not reach all the elements of Z_7^*.
- The order of an element $g \in Z_p^*$ is the smallest positive integer a such that $g^a = 1 \mod p$. The order of $g \in Z_p^*$ is denoted by $\mathrm{ord}_p(g)$.

  Example: $\mathrm{ord}_7(3) = 6$ and $\mathrm{ord}_7(2) = 3$.
- Lagrange's theorem says that for all $g \in Z_p^*$ we have that $\mathrm{ord}_p(g)$ divides $p-1$.

1.3 Quadratic residues

- Quadratic residues are a subgroup of Z_p^*.
- The square root of $x \in Z_p$ is a number $y \in Z_p$ such that $y^2 = x \mod p$
  - Example: $\sqrt{2} \mod 7 = 3$ because $3^2 = 2 \pmod 7$.
  - $\sqrt{3} \mod 7$ does not exist.
- An element $x \in Z_p^*$ is a quadratic residue if it has a square root in Z_p.

- How do we test whether an element is a quadratic residue?
  - The Legendre symbol for an element $x \in Z_p^*$ is defined as

$$\left(\frac{x}{p}\right) = \begin{cases} 1 & \text{if } x \text{ is a QR in } Z_p \\ 2 & \text{if } x \text{ is not a QR in } Z_p \\ 0 & \text{if } x = 0 \mod p \end{cases} \tag{1}$$

  - By Euler's theorem, $\left(\frac{x}{p}\right) = x^{\frac{p-1}{2}} \mod p$, so the Legendre symbol can be efficiently computed.
  - Let g be a generator of Z_p^*. x is a quadratic residue if it's discrete log with respect to g is even. That is, for y such that $g^y = x$, $y = 2k$ for some integer k
  - So if x is a quadratic residue, $x^{\frac{p-1}{2}} = g^{2k\frac{p-1}{2}} = g^{k(p-1)} = 1 \pmod p$

1.4 Easy and hard problems

- An easy problem is one that can be solved in time polynomial to the length of the input. Easy problems in Z_p^*:
  - Adding and multiplying elements.
  - Computing g^r, even if r is large (using repeated squaring).
  - Inverting an element.
  - Testing if an element is a QR or not.
- Believed to be hard in Z_p^*:
  - Discrete log problem.
  - Computational Diffie Hellman (CDH) problem.

1.5 Exercises

1. Let $p = 2q + 1$ be a "safe prime" (where q is prime). Clearly any quadratic residue $x = a^2 \pmod p$ is not a generator of Z_p^*, since its powers are also squares. Give a counterexample to the conjecture that any any non-quadratic-residue in Z_p^* other than 1 is a generator of Z_p^*.

   Solution: The possible orders of elements in Z_p^* are 1, 2, q, and $p - 1 = 2q$, and there are elements of each such order. The quadratic residues are 1 and those elements of order q. The element of order 2 (i.e. -1) will not be a generator of Z_p^*. Thus, -1 is a counterexample, since it only generates $\{-1, 1\}$.

2. Argue that if g is a generator of Z_p^*, where p is prime, and if k is relatively prime to $p - 1$, then g^k is also a generator of Z_p^*.

   Solution: Note that g has order $p-1$, and that k has an inverse ℓ modulo $p-1$, so that $(g^k)^\ell = g$, and powers of g^k are just powers of g, since $(g^k)^{\ell t} = (g^{k\ell})^t = g^t$; thus powers of g^k include all powers of g.

3. Consider the Diffie-Helman key exchange protocol over the group $G = Z_p^*$, where p is a large prime number (say a 2048-bit prime), and where g is a generator of Z_p^*. Alice sends $g^a \mathsf{~mod~} p$ and Bob sends $g^b \mathsf{~mod~} p$, where a, b are random in $\{1, \ldots, p-1\}$. The secret is $K = g^{ab} \mathsf{~mod~} p$. Does this scheme have strong security? Namely, is K indistinguishable from a random element in Z_p^* given $g^a \mathsf{~mod~} p$ and $g^b \mathsf{~mod~} p$?

Solution: No. For example if one of the messages is a QR (quadratic residue) then the key must be a QR. (This was in lecture as well)

2 Practice problems

2.1 Example: Weak SPA security.

Define "weak CPA security" (WCPA) of a conventional (non-public-key) encryption scheme $\texttt{Enc}(k, \cdot)$ as for CPA security, except that the Challenger can only ask for the encryption of *random* messages. That is, the Challenger may ask for, and receive, pairs of the form $(r, \texttt{Enc}(k, r))$ where r has been uniformly and randomly chosen. Argue that an encryption scheme may be WCPA secure but not CPA secure.

Solution: Suppose that Enc has the property that feeding it a message of 0 gives the key k as output, but is otherwise CPA secure if the message 0 is never input. This scheme is WCPA secure but not CPA secure, since the CPA Challenger could ask for an encryption of 0.

2.2 Example: Block cipher.

Let $\texttt{Enc}(k, m)$ denote a given block cipher that takes as input an n–bit key k and an n–bit message block m, and returns an n–bit ciphertext block $c = \texttt{Enc}(k, m)$. In this problem you may assume that Enc is an ideal block cipher.

Define a new block cipher $\texttt{Enc}'((k_1, k_2), m)$ in terms of Enc as follows. The block cipher $\texttt{Enc}'$ takes as input a key k consisting of *two* n-bit key-parts k_1 and k_2, and an n-bit message block m, and returns the $2n$-bit ciphertext block

$$c = (c_1, c_2) = \texttt{Enc}'((k_1, k_2), m) = \texttt{Enc}(k_1, r) \,||\, \texttt{Enc}(k_2, s)$$

where r and s are random values that add to m modulo 2^n. That is, the result is the concatenation of the encryption of a random n–bit value r under Enc using key k_1 and the encryption of $s = m - r$ under Enc using key k_2. Arithmetic is modulo 2^n, so that $r + s = m \pmod{2^n}$.

(a) Is $\texttt{Enc}'$ a CPA–secure block cipher? Explain.

Solution: Yes. $\texttt{Enc}(k_1, r)$ and $\texttt{Enc}(k_2, s)$ are essentially fresh random values that say nothing about m.

(b) Is $\texttt{Enc}'$ a CCA–secure block cipher? Explain.

Solution: No. The challenger, before receiving an encryption (c_1, c_2) of an unknown message m, can obtain an encryption (c_1', c_2') of the message 0. The decryption oracle will allow the challenger to decrypt the ciphertext (c_1, c_2') (yielding m_1), and the ciphertext (c_1', c_2) (yielding m_2). The sum $m_1 + m_2 \pmod{2^n}$ is equal to the target message m. We can ignore the negligible chance that (c_1, c_2) is equal to either of (c_1, c_2') or (c_1', c_2).

2.3 Example: Symmetric cryptography in the random oracle model.

Suppose you are in a world in which there is access to a random oracle $\mathcal{H}$. With no other assumptions, which of the following can you construct? For each, either give your construction or argue why it cannot be constructed from $\mathcal{H}$. (Tip: pay careful attention to the use of any keys.)

(a) A pseudo–random function $F(k, \cdot)$.

(b) A CPA–secure symmetric encryption scheme.

(c) A secure message authentication code.

(d) A CCA–secure symmetric encryption scheme.

Solution: They can all be constructed! Access to $\mathcal{H}$ is very powerful since it true randomness, and therefore it is pseudo–random, one–way, and collision resistant. Consider the following:

(a) Set $F(k, \cdot) = \mathcal{H}(k||\cdot)$.

(b) A CPA–secure encryption scheme follows from a PRF. Here we assume that $|m| = |\mathcal{H}(k||r)$.

$$
\begin{array}{ll}
\texttt{Gen}(1^n): & \text{output } k \xleftarrow{\$} \mathcal{K} \\
\texttt{Enc}(k, m): & \text{sample random } r \\
 & \text{output } c = (r, \mathcal{H}(k||r) \oplus m) \\
\texttt{Dec}(k, c): & \text{compute } \omega = \mathcal{H}(k||r) \text{ and output } \omega \oplus c[2] = m.
\end{array}
$$

(c) A message authentication code also follows from a PRF: $\texttt{MAC}(k, m) = \mathcal{H}(k||m)$.

(d) With (b) and (c), a CCA–secure encryption scheme is given as:

$$
\begin{array}{ll}
\texttt{Gen}(1^n): & \text{output } k_c, k_i \xleftarrow{\$} \mathcal{K} \\
\texttt{Enc}(k_c, k_i, m): & \text{sample random } r \\
 & \text{output } c = (r, \mathcal{H}(k_c||r) \oplus m) \text{ and } t = \mathcal{H}(k_i||c[2]) \\
\texttt{Dec}(k_c, k_i, c, t): & \text{compute } \nu = \mathcal{H}(k_i||c[2]) \\
 & \text{if } \nu = t, \text{ compute } \omega = \mathcal{H}(k_c||r) \text{ and output } \omega \oplus c[2] = m \\
 & \text{else, output } \perp.
\end{array}
$$

The keys are named k_c for confidentiality and k_i for integrity.

2.4 Example: Domain Extension

Suppose you are given a MAC scheme with message space $\{0,1\}^{128}$ that generates a MAC in $\{0,1\}^{128}$. Show how you can convert this MAC scheme into one with message space $\{0,1\}^{256}$, while maintaining security. *hint: You can think of the* MAC *as being a* PRF

Solution: The new MAC will have 2 MAC keys (k, k'). To MAC a message (m_1, m_2) compute $t_1 = MAC(k, m_1)$ then compute $t_2 = MAC(k, t_1 \oplus m_2)$ and outputs $MAC(k', t_2)$

3 References

Number theory handout: https://crypto.stanford.edu/ dabo/cs255/handouts/numth1.pdf
6.857 past quizzes