MAT 302: ALGEBRAIC CRYPTOGRAPHY

Department of Mathematical and Computational Sciences
University of Toronto, Mississauga

February 27, 2013

Mid-term Exam

INSTRUCTIONS:

- The duration of the exam is 100 minutes.
- The exam is worth a total of 100 marks.
- This booklet has 14 pages (excluding the title page) and 5 questions.
- Please use the workspace at the end of this booklet for calculations. Ask for extra sheets of paper if needed.
- You are allowed to bring one 3" × 5" cue ('index') card to the exam with writing on both sides. No other written notes are permitted.
- No Calculators, Cellphones, Laptops or other electronic devices.

Good luck!

QUESTIONS

Problem 1 (10 Marks)

Please circle the correct answer. You don't have to show your work, although that might fetch you partial marks.

- How many solutions does the equation $x^2 = 1 \pmod{30}$ have?

  (A) 1 (B) 2 (C) 4 (D) 8 (E) None of the above

  Answer: (C).
  The number of solutions to $x^2 = 1 \pmod{2}$ is 1.
  The number of solutions to $x^2 = 1 \pmod{3}$ is 2.
  The number of solutions to $x^2 = 1 \pmod{5}$ is 2.
  By Chinese remaindering, any combination of solutions mod 2, 3 and 5 gives us a distinct solution mod 30. Thus, there are 4 solutions.

- How many elements of $\mathbb{Z}_{29}^*$ are generators?

  (A) 28 (B) 6 (C) 12 (D) 14 (E) None of the above

  Answer: (C).
  The number of generators of $\mathbb{Z}_p^*$ is $\phi(p-1)$ if p is prime. Thus, we have $\phi(28) = 12$ generators.

Problem 2 (20 Marks)

Compute the last two digits of $99^{523^{425}}$. Show your work.

Answer: We have to compute $99^{523^{425}} \pmod{100} = (-1)^{523^{425}} \pmod{100}$. Since the exponent is clearly odd, this is $-1 \pmod{100} = 99 \pmod{100}$. The last two digits are 99.

Problem 3: Crypto (25 Marks)

1. **(15 Marks)** Write down the El Gamal encryption scheme. Make sure to specify what the public and secret keys are, and how the encryption and decryption algorithms work.
   `[If you don't know the answer to this and still want to attempt part (2), you can get ask Serge for the answer to part (1), but then of course you won't get any points for part (1).]`

   Answer: Refer to your course notes.

2. **(10 Marks)** Show that the El Gamal scheme is multiplicatively homomorphic. That is, given encryptions of two messages M_1 and M_2, you can construct an encryption of their product M_1M_2 (without knowing the secret key, of course).

   Answer: The El Gamal ciphertext of a message M using public key $PK = (g, g^x, p)$ and randomness r is the pair $(g^r \pmod p, g^{rx} \cdot M \pmod p)$. *Note that every time you encrypt a message under public key PK, you choose a new random number r for encryption.*

   Given a ciphertext $(g^{r_1} \pmod p, g^{r_1 x} \cdot M_1 \pmod p)$ of message M_1 and a ciphertext $(g^{r_2} \pmod p, g^{r_2 x} \cdot M_2 \pmod p)$ of message M_2, compute their element-wise product, namely,

$$\left[(g^{r_1} \cdot g^{r_2}, (g^{r_1 x} \cdot M_1) \cdot (g^{r_2 x} \cdot M_2)\right] = \left[g^{r_1+r_2}, g^{(r_1+r_2)x} \cdot (M_1 M_2)\right]$$

   which is an encryption of the product M_1M_2 (using randomness $r_1 + r_2$.)

   The point is that when you decrypt this new ciphertext using the secret key x, what you get is exactly the product M_1M_2.

Problem 4: Fermat, Witnesses and Liars (20 Marks)

1. **(5 Marks)** Let N be a natural number. What is the definition of the set of Fermat Witnesses mod N? How about Fermat Liars?

   Answer: For a composite number N, the Fermat Liars FL_N are defined as follows:

   $$FL_N = \{x \in \{0, 1, \ldots, N-1\} : \ \mathsf{gcd}(x, N) = 1 \text{ and } x^{N-1} = 1 \pmod{N}\}$$

   the set of Fermat Witnesses FW_N is defined as follows:

   $$FW_N = \{x \in \{0, 1, \ldots, N-1\} : \ \mathsf{gcd}(x, N) = 1 \text{ and } x^{N-1} \neq 1 \pmod{N}\}$$

2. **(10 Marks)** What are the Fermat Witnesses and Liars mod 15?

   Answer: 1 and $-1 \pmod{15} = 14 \pmod{15}$ are clearly Fermat Liars.

   By computation, we find that 4 and $-4 \pmod{15} = 11 \pmod{15}$ are also Fermat Liars since $4^{14} = 11^{14} = 1 \pmod{15}$.

3. **(5 Marks)** What are the Miller-Rabin Liars mod 15?
`[Hint: Solve Part (2) first]`

Answer: Clearly, the Miller Rabin Liars are a subset of the Fermat Liars. The Miller Rabin liars are those x which are Fermat Liars and in addition, $x^2 \neq 1 \pmod{N}$.

Since $4^2 = 11^2 = 1 \pmod{15}$, 4 and 11 are both Miller Rabin witnesses. The MR liars are 1 and 14.

Problem 5: Generators (25 Marks)

Let $p > 3$ be prime, and let $g_1, \ldots, g_m$ be the generators of $\mathbb{Z}_p^*$. Prove that their product is 1 mod p. That is, prove that

$$\prod_{i=1}^{m} g_i = 1 \pmod{p}$$

Answer: We prove two claims.

First, we claim that if g is a generator of $\mathbb{Z}_p^*$, then so is g^{-1}. For if $(g^{-1})^k = 1 \pmod{p}$, then $g^k = 1 \pmod{p}$ as well, meaning that the powers of g^{-1} that evaluate to 1 are precisely the power of g that evaluate to 1. Since the smallest non zero power of g that evaluates to 1 is $p-1$, the smallest non zero power of g^{-1} that evaluates to 1 is also $p-1$ meaning that g^{-1} is a generator as well.

Secondly, we claim that $g \neq g^{-1}$. If not, that would mean that $g^2 = 1 \pmod{p}$. This contradicts the fact that g is a generator for any $p > 3$.

Put together, we can partition the set of generators into pairs (g_i, g_i^{-1}) where the two elements in each pair are distinct. Thus,

$$\prod_{i=1}^{m} g_i = \prod (g_i \cdot g_i^{-1}) = 1 \pmod{p}$$

WORK SHEET

WORK SHEET

WORK SHEET