

MATH 110 SAMPLE MIDTERM

Friday, May 20, 2005

Name: _____

Numeric Student ID: _____

I agree to abide by the terms of the honor code:

Signature: _____

Instructions: Print your name, and student ID number in the space provided. You may not use notes, or textbooks, or calculators. Read each question carefully. As ever, try to be as precise as possible when writing your proofs. Correct answers without justification will receive little or no credit. There are 6 questions. There is an 80 minute time limit on this exam. Good luck.

Question	Score	Maximum
1		10
2		10
3		10
4		10
5		10
6		10
Total		60

1. (a) Find all primitive elements in $(\mathbb{Z}/11\mathbb{Z})^\times$

(b) In the integers mod 17, 3 is a primitive root. Use the following table of indices to solve the subsequent equations for all $x \pmod{17}$.

a (mod 17)	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
i(a) (mod 16)	16	14	1	12	5	15	11	10	2	3	7	13	4	9	6	8

i. $x^4 \equiv 1 \pmod{17}$

ii. $7x^{11} + 5 \equiv 0 \pmod{17}$

2. Consider the RSA cryptosystem with public key $(m, e) = (77, 7)$.

(a) Encode the number 4.

(b) This cryptosystem, as you may have noticed, is not secure. Decode the ciphertext 3.

(c) Explain why, in general, RSA is not secure if the two primes p, q such that $pq = m$ are chosen to be of the same size. That is, provide an algorithm for breaking this cryptosystem.

3. Abner (A) and Barbara (B) decide to use the Diffie-Hellman key exchange to agree on a secret key, which you must intercept. As a serious affront to your cryptoanalytic abilities, they agree on a prime modulus 13 and a primitive element 2. If Abner sends 6 to Barbara, who sends 11 back to Abner, what is their secret key?

4. (a) Construct the finite field \mathbb{F}_{49} by writing it in the form $\mathbb{F}_7/(p(x))$ for some irreducible polynomial $p(x)$.

(b) How many different choices of $p(x)$ are there which produce this field?

(c) Find a generator for $(\mathbb{F}_{49})^\times$ (and prove that this is a generator).

5. Let E be the elliptic curve $E : y^2 = x^3 + 1$. The coefficient 1 may be considered to live in the rationals, mod p , or as the multiplicative identity in a finite field.

(a) Find three points of E over the finite field \mathbb{F}_7

(b) Find a point of E over the finite field $\mathbb{F}_{25} = \mathbb{F}_5[x]/(x^2 + 2)$

(c) Show that the five points $(-1,0)$, $(0,1)$, $(0,-1)$, $(2,3)$, and $(2,-3)$ with the point O at infinity form a group of size 6 under addition of points on an elliptic curve. (That is, check closure of this set under elliptic curve addition and check that each point has an additive inverse.)

6. A quadratic residue mod n is a number a such that

$$x^2 \equiv a \pmod{n}$$

Show that in $(\mathbb{Z}/p\mathbb{Z})^\times$, the number of quadratic residues mod p is always equal to the number of quadratic non-residues mod p (that is, numbers $a \pmod{p}$ without such a solution).