Math 406 Exam 3 Summer 2016

Directions: Each numbered question is worth ten points. Coherent, logical justification (including words and clear calculations) is required for all problems except those in which counterexamples are requested, those can just be given, or for simple computations.

Note: I've ordered these by difficulty as I perceive it. Your opinion on difficulty might vary, but knowing how I ordered them might help you decide which to do first and which to do last!

1. Evaluate each of the following:

   (a) $\left(\frac{19}{45}\right)$

   (b) $\left(\frac{1001}{9907}\right)$

2. A partial table of indices for 2, a primitive root of 13, is given here:

a	1	2	3	4	5	6	7	8	9	10	11	12
$\text{ind}_2 a$	12	1	4	2	9	5	11	3	a	b	7	6

   (a) Find a and b with justification.

   (b) Use the table to solve the congruence $3^{2x+1} \equiv 9 \bmod 13$.

   (c) Use the table to solve the congruence $7x^5 \equiv 3 \bmod 13$.

3. For each $1 \leq a \leq 15$ with $\gcd(a, 15) = 1$ find and justify $\text{ord}_{15} a$.

4. Suppose that Bob's public key is $(e, n) = (3, 33)$.

   (a) Encrypt the message `CAFE` using 1-character blocks.

   (b) Since you are so smart you can factor n and find $\phi(n)$. Do so, then calculate Bob's private key d.

   (c) Decrypt the single ciphertext `04`.

5. The ciphertext `MOOHCHHXBOO` was created using an affine cipher. Perform frequency analysis and decrypt.

6. Determine whether 15 is a quadratic residue of 17:

   (a) Using Euler's Criterion.

   (b) Using Gauss' Lemma.

7. Prove that if $\text{ord}_n a = hk$ then $\text{ord}_n \left(a^h\right) = k$.

8. Let r be a primitive root for an odd prime p. Prove that $\text{ind}_r(p-1) = \frac{1}{2}(p-1)$.

9. Suppose p and q are distinct odd primes. Prove that there is always some n with $\left(\frac{n}{pq}\right) = -1$.

10. Suppose p is an odd prime such that there is some a so that a is a quadratic residue of p but $2a$ is a quadratic non-residue of p. Prove that $p \equiv \pm 3 \bmod 8$.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

The End