MATH 42
MIDTERM 2
20 MARCH 2015

Name : ____

- The time limit is 50 minutes.
- No calculators or notes are permitted.
- Each problem is worth 5 points.

1	/5	**2**	/5
3	/5	**4**	/5
5	/5	**6**	/5
		$\sum$	/30

(1) When the students in a classroom divide into groups of nine, there are four students left over. When the students break into groups of eleven, there is one student left over. Assuming that there are fewer than 100 students in the room, how many students must there be?

(2) What is the remainder when 10^{100} is divided by 19?

(3) (a) How many numbers between 1 and 1500 inclusive are relatively prime to 1500 (that is, share no common factors besides 1 with 1500)?

(b) Find the remainder when 1493^{2002} is divided by 1500.

(4) Suppose that Bob's RSA public key is $(33, 13)$. Alice sends Bob the cipher text $c = 8$. What was Alice's plain text?
(Recall that if s is Alice's plain text, then she computes the cipher text c by computing the remainder when s^{13} is divided by 33.)

(5) (a) Let p be an *odd* prime (i.e. a prime besides 2), and k be a positive integer. Prove that if $a^2 \equiv 1 \pmod{p^k}$, then either $a \equiv 1 \pmod{p^k}$ or $a \equiv -1 \pmod{p^k}$.

(b) Find all integers a between 1 and 63 inclusive such that $a^2 \equiv 1 \pmod{64}$.

(6) Let $d(n)$ denote the number of divisors of n, including 1 and n. For example:

$$\begin{aligned} d(10) &= 4 \text{ (the divisors are } 1, 2, 5, 10) \\ d(17) &= 2 \text{ (the divisors are } 1, 17) \\ d(24) &= 8 \text{ (the divisors are } 1, 2, 3, 4, 6, 8, 12, 24) \end{aligned}$$

You may assume the following fact: if $\gcd(m, n) = 1$, then $d(mn) = d(m)d(n)$ (I encourage you to try to prove it, but you don't need to do it now).

(a) Find a formula for $d(p^k)$, where p is prime and $k \geq 1$.
(b) Compute $d(91000)$.
(c) Give a simple criterion to tell whether $d(n)$ is even or odd.

(additional space for work)