Mathematics 312, Section 101. Final Exam

December 17, 2010. Instructor: Z. Reichstein.

This is a closed book exam. You can use one 8.5" $\times$ 11" note sheet. No other materials or calculators are allowed. In order to receive credit for a problem you need to show enough work to justify your answer.

Name (Please print):

Student number:

Problem	**Score**	**Problem**	**Score**
1		5	
2		6	
3		7	
4		8	

TOTAL

Problem 1 (7 marks). Let n be an integer. Show that there does not exist a prime number $p \geq 2$ which divides both $8n + 3$ and $5n + 2$.

Problem 2 (6 marks). Let $n = 3^{100}$ and $a = 8585\dots85$ be the $2n$-digit number, where the digits 85 repeat n times.

(a) Is a divisible by 9?

(b) Is a divisible by 11?

Explain your answers.

Problem 3 (7 marks). Find all three-digit combinations that can occur as the last three digits of a^{100}, where a ranges over the integers. Give a simple criterion for predicting which of these possibilities occurs for a given a, without computing a^{100}. Prove that your criterion is correct.

Hint: Investigate a^{100} modulo 8 and modulo 125 separately, then use the Chinese Remainder Theorem.

Problem 4 (6 marks). Suppose a positive integer n has 77 positive divisors (1 and n count among them). How many of these divisors can be primes? Explain your answer.

Problem 5 (6 marks). Find all positive integers n such that $\phi(n) = 22$ and prove that there are no others. Here ϕ denotes the Euler ϕ-function.

Problem 6 (6 marks). Recall that an affine cryptosystem, with encryption key $K_E = (26, a, b)$ and decryption key $K_D = (26, c, d)$ works as follows. Each letter is assigned a numerical value, in alphabetical order: $A \mapsto 0$, $B \mapsto 1$, ..., $Z \mapsto 25$. These numbers are then viewed modulo 26; they are encrypted by the formula

$$x \longrightarrow y \equiv ax + b \pmod{26}$$

and decrypted by the formula

$$y \longrightarrow x \equiv cy + d \pmod{26}.$$

It is known that the most frequently occurring letter in the English language is E (with numerical value 4) and the second most frequently occurring letter is T (with numerical value 19). Suppose these letters are encoded as F (numerical value 5) and G (numerical value 6), respectively.

(a) Find the encryption key K_E.

(b) Find the decryption key K_D.

Problem 7 (6 marks). Suppose the public key for an RSA cryptosystem is $(n, e) = (85, 7)$ and the secret key is $(85, d)$. Show that this cryptosystem is not secure by finding d.

Remarks: Recall that a message x is encoded by $x \longrightarrow x^e \pmod n$ and a received message y is decoded by $y \longrightarrow y^d \pmod n$. To make this cryptosystem secure, one needs to use a much larger n.

Problem 8 (6 marks). Prove that the congruence $x^5 \equiv 1 \pmod{52579}$ has exactly one solution, $x \equiv 1 \pmod{52579}$. Use the fact that 52579 is a prime. What other property of 52579 is used in your proof?