Lecture 15: Midterm

William Stein

Math 124 Harvard University **Fall 2001**

Contents

1 Introduction

The midterm examination took place on October 17 at 11AM. Twenty two students had 52 minutes to do complete all of these problems with no external aids such as a calculator or notes. Happily, 11 students earned A's (with 3 perfect scores!); unfortunately, 7 students received a D.

2 The Midterm Exam

Justify your answers. If you do a computation by "pure thought", explain those pure thoughts.

1. (5 points) Prove that a positive number n is divisible by 11 if and only if the alternating sum of the digits of n is divisible by 11.

2. Let $\varphi : \mathbb{N} \to \mathbb{N}$ be the Euler φ function.

   (i) (3 points) Find all natural numbers n such that $\varphi(n) = 1$.

   (ii) (2 points) Do there exist natural numbers m and n such that $\varphi(mn) \neq \varphi(m) \cdot \varphi(n)$?

3. (6 points) Nikita and Michael decide to agree on a secret encryption key using the Diffie-Hellman key exchange protocol. You observe the following:

   - Nikita chooses $p = 13$ for the modulus and $g = 2$ as generator.
   - Nikita sends 6 to Michael.

- Michael sends 11 to Nikita.

What is the secret key?

4. Consider the RSA public-key cryptosystem defined by $(n, e) = (77, 7)$.

   (i) (3 points) Encrypt the number 4 using this cryptosystem.

   (ii) (3 points) Find an integer d such that $ed \equiv 1 \pmod{\varphi(n)}$.

5. (5 points) How many natural numbers $x < 2^{13}$ satisfy the equation

$$x^2 \equiv 5 \pmod{2^{13} - 1}?$$

   (You may assume that $2^{13} - 1$ is prime.)

6. (10 points) Which of the following systems of equations have at least one solution? Briefly justify your answers.

   (a) $\begin{aligned} x &\equiv 1 \pmod 3 \\ x &\equiv -1 \pmod 9 \end{aligned}$

   (b) $2x \equiv 1 \pmod{123456789101112131415 1}$

   (c) $\begin{aligned} x^2 &\equiv 5 \pmod{29} \\ x^2 &\equiv 3 \pmod{47} \end{aligned}$

   (d) $\begin{aligned} x &\equiv 3 \pmod{29} \\ x &\equiv 5 \pmod{47} \end{aligned}$

   (e) $\begin{aligned} x^2 &\equiv 3 \pmod{29} \\ x^2 &\equiv 5 \pmod{47}. \end{aligned}$

7. (5 points) Find the natural number $x < 97$ such that $x \equiv 4^{48} \pmod{97}$. (You may assume that 97 is prime.)

3 Abbreviated Solutions

1. We use that $10 \equiv -1 \pmod{11}$ and facts about modular arithmetic. Write $n = \sum_{i=0}^{r} d_i 10^i$. Then $n \equiv \sum_{i=0}^{r} (-1)^i d_i \pmod{11}$, so $n \equiv 0 \pmod{11}$ if and only if the alternating sum of the digits $\sum (-1)^i d_i$ is congruent to 0 modulo 11.

2. For the first part, the answer is $\mathbf{n = 1, 2}$. On a previous homework we proved that $n = 1, 2$ are the only n such that $\varphi(n)$ is odd. For the second part, the fact that φ is multiplicative means that if $\gcd(m, n) = 1$ then $\varphi(mn) = \varphi(m) \cdot \varphi(n)$. When $\gcd(m, n) \neq 1$ this implication can fail; for example,
$$2 = \varphi(2 \cdot 2) \neq \varphi(2) \cdot \varphi(2) = 1.$$

3. Since $2^n \equiv 6 \pmod{13}$, a table of powers of 2 modulo 13 quickly reveals that n must be 5 (we solve the discrete log problem easily in this case since 13 is so small). Likewise, since $g^m \equiv 11 \pmod{13}$ we see that $m = 7$. The secret key is $\mathbf{s = 7}$ since $g^{nm} = 2^{35} \equiv 2^{11} \equiv 7 \pmod{13}$. (Some people who attempted this problem incorrectly thought the secret key should be $g^n \cdot g^m = g^{n+m}$.)

4. (a) We must compute $4^7 \pmod{77}$. Working modulo 77, we have that
$$4^7 = 64 \cdot 64 \cdot 4 = 13^2 \cdot 4 = 169 \cdot 4 = 15 \cdot 4 = 60,$$
so 4 encrypts as **60**.
   (b) First, $\varphi(n) = \varphi(77) = \varphi(7) \cdot \varphi(11) = 6 \cdot 10 = 60$. (Some people incorrectly thought that $\varphi(n) = 77$ for some reason.) We then use the extended Euclidean algorithm to find an integer e such that $7e \equiv 1 \pmod{60}$. We find that $2 \cdot 60 - 17 \cdot 7 = 1$, so $\mathbf{e = -17}$ is a solution.

5. First we use the law of quadratic reciprocity to decide whether or not there is a solution. We have
$$\left(\frac{5}{2^{13}-1}\right) = (-1)^{2 \cdot (2^{13}-2)/2} \left(\frac{2^{13}-1}{5}\right) = \left(\frac{1}{5}\right) = 1,$$
so the equation $x^2 \equiv 5 \pmod{2^{13}-1}$ has at least one solution a. Since the polynomial $x^2 - 5$ has degree two and $2^{13} - 1$ is prime, there are at most 2 solutions. Since $-a$ is also a solution and $a \neq 0$, there are **exactly two solutions**.

6. (a) has **no solutions** because $x \equiv -1 \pmod{9}$ implies that $x \equiv -1 \pmod{3}$. (b) has **a solution** because $\gcd(2, 12345678910111213141 51) = 1$. (c) has **a solution** because $\left(\frac{5}{29}\right) = \left(\frac{3}{47}\right) = 1$ so there are a and b such that $a^2 \equiv 5 \pmod{29}$ and $b^2 \equiv 3 \pmod{47}$; the Chinese Remainder Theorem then implies that there is an x such that $x \equiv a \pmod{29}$ and $x \equiv b \pmod{47}$. (d) has **a solution** by the Chinese Remainder Theorem, since $\gcd(29, 47) = 1$. (e) has **no solution** since $\left(\frac{3}{29}\right) = -1$, so the first of the two equations doesn't even have a solution.

7. Since 97 is prime, Fermat's Little Theorem implies that $4^{48} = 2^{96} \equiv \mathbf{1} \pmod{97}$.