

MATH 5405 - HW1

DUE 01/26/2009

The purpose of this HW is to review mathematics of MATH 4400. In particular, the background material is in the notes.

- 1) Use Euclidean Algorithm to find the greatest common divisor of
 - a) 1084 and 412.
 - b) 1979 and 531.
 - c) 305 and 185.
- 2) The number 0-251-32133-6 is obtained by transposing two consecutive digits of a valid ISBN number. Find that ISBN number. Recall that the digits of a valid ISBN number $x_1 - x_2x_3x_4 - \dots$ satisfy the congruence

$$\sum_{i=1}^{10} ix_i \equiv 0 \pmod{11}.$$

- 3) Use the Euclidean Algorithm to compute the multiplicative inverse of
 - a) 131 modulo 1979.
 - b) of 127 modulo 1091.
- 4) Use the previous exercise to solve the following congruences:
 - a) $131x \equiv 99 \pmod{1979}$.
 - b) $127x \equiv 85 \pmod{1091}$.
- 5) Let G be a group and g an element in G of order n . Let m be a positive integer such that $g^m = e$. Show that n divides m . Hint: write $m = qn + r$ with $0 \leq r < n$.
- 6) Build the first 12 rows of the Pascal triangle modulo 11.
- 7) Find the inverse of $2 + 5i$ modulo 31. Is there an inverse of $2 + 5i$ modulo 29? Explain.
- 8) The number 2 is a primitive root modulo 19. Compute the powers 2^I for $I = 1, 2, \dots, 18, 19$ to obtain the table for the discrete logarithm with base 2 for integers modulo 19. Then use the table to solve the equation

$$x^5 \equiv 7 \pmod{19}.$$

- 9) Let p be a prime congruent to 1 modulo 8 and g a primitive root modulo p . Then

$$s = g^{\frac{p-1}{8}} + g^{\frac{7(p-1)}{8}}$$

is square root of 2. Compute s and verify that $s^2 \equiv 2 \pmod{p}$ in the following two cases:

- 1) $p = 41$ and $g = 6$.
- 2) $p = 73$ and $g = 5$.

10) Let p be a prime congruent to 1 modulo 3 and g a primitive root modulo p . Then

$$t = g^{\frac{p-1}{3}} - g^{\frac{2(p-1)}{3}}$$

is square root of -3 . Compute t and verify that $t^2 \equiv -3 \pmod{p}$ in the following two cases:

- 1) $p = 43$ and $g = 3$.
- 2) $p = 73$ and $g = 5$.