MATH 540: GUIDELINES AND PRACTICE PROBLEMS FOR EXAM 2

Exam 2 will cover all material presented in class since Exam 1 up to and including whatever we covered on Thursday April 10. Questions on the exam will be of the following types: Stating definitions, propositions or theorems; short answer; true-false; and presentation of a proof of a theorem. Though the proofs you are responsible for are listed below, you will be responsible for verifying various theorems in class for particular examples. You **will** be allowed to use a calculator on this exam.

Any definitions, propositions theorems, corollaries that you need to know how to state appear in the Daily Update, and all such are candidates for questions. You will need to be able to answer brief questions about these results as well as true-false statements about these results. Most of the definitions you need to know are also in the Daily Update, but it is best to check your notes for all definitions we have given by February 20.

You will also be responsible for working any type of problem that was previously assigned as homework.

On the Exam you will be required to state and provide a proof of one of the following Theorems.

(i) Be able to state the Chinese Remainder Theorem in full generality, but provide a proof when just two congruences are given.
(ii) Euler's Quadratic residue Theorem
(iii) The existence of a division algorithm for the Gaussian integers

Practice Problems

1. Solve the system of congruences

$$x \equiv 6 \bmod 7$$
$$x \equiv 4 \bmod 6$$
$$x \equiv 10 \bmod 11$$

2. Find the primitive roots of 1 mod 7 and mod 11. Find an integer n other than 8 for which there are no primitive roots of one modulo 8.

3. Solve the quadratic congruence $5x^2 + 3x + 1 \equiv 0 \bmod 17$. Give an example of a quadratic equation $f(x) = 0$ and a prime p such that $p(x) \equiv \bmod p$ does not have a solution.

4. Use the definitions and properties in class to calculate $(\frac{3}{16})$, $(\frac{5}{101})$, $(\frac{1{,}000{,}001}{17})$, $(\frac{-48}{101})$.

5. Use Euler's theorem to find the quadratic residues modulo 19.

6. Calculate $(\frac{5}{31})$, using Gauss's Lemma.

7. Verify the Numerical Lemma from the lecture of April 3, for $p = 5, q = 11$, first by using the formula, and then by counting in two ways the lattice points strictly contained in the rectangle $(0,0), (\frac{5}{2}, 0), (\frac{5}{2}, \frac{5}{2}, \frac{11}{2}), (0, \frac{11}{2})$.

8. Find a GCD of $x = 8 + 6i$ and $y = 3 - 4i$ in the Gaussian integers.

Math 540 Sol^{ns} to Exam 2 practice problems

1. Set $N = 7 \cdot 6 \cdot 11 = 462$,

$$N_1 = \frac{462}{7} = 66, \quad N_2 = \frac{462}{6} = 77, \quad N_3 = \frac{462}{11} = 42$$

$66 \equiv 3 \bmod 7$ and $c_1 \equiv 5 \bmod 7$ is the inverse of 3

$77 \equiv 5 \bmod 6$ and $c_2 \equiv 5 \bmod 6$ is the inverse of 5

$42 \equiv 9 \bmod 11$ and $c_3 \equiv 5 \bmod 11$ is the inverse of 9

Then $x = 6 \cdot 5 \cdot 66 + 4 \cdot 5 \cdot 77 + 10 \cdot 5 \cdot 42 \Rightarrow$

$x \equiv 76 \bmod 462$

2. For primitive roots mod 7, we want non-zero elts $a \bmod 7$ s.t. $a^6 \equiv 1 \bmod 7$, but no smaller r satisfies $a^r \equiv 1 \bmod 7$

Answer: 3, 5

For prim. roots mod 11: 2, 6, 7, 8

3. Actually: no root mod 17 since $b^2 - 4ac = -11 \equiv 6 \bmod 17$ and 6 is not a square mod 17

4.
$$\left(\frac{3}{16}\right) = \left(\frac{3}{2}\right)^4 = \left(\frac{1}{2}\right)^4 = 1$$

$$\left(\frac{5}{101}\right) = (-1)^{2 \cdot 50}\left(\frac{101}{5}\right) = \left(\frac{1}{5}\right) = 1$$

$$\left(\frac{11{,}000{,}001}{17}\right) = \left(\frac{10}{17}\right) = \left(\frac{2}{17}\right)\left(\frac{5}{17}\right) = (-1)(-1) = 1$$

$$\left(\frac{-48}{101}\right) = \left(\frac{53}{101}\right) = (-1)^{26 \cdot 50}\left(\frac{101}{53}\right) = \left(\frac{48}{53}\right) = \left(\frac{2}{53}\right)^4 \cdot \left(\frac{3}{53}\right) = (-1)^4(-1) = -1$$

5. We seek $1 \le a \le 18$ st $a^{\frac{19-1}{2}} \equiv 1 \mod 19$

Answers: 1, 4, 5, 6, 7, 9, 11, 16, 17

Since $1^{18} \equiv 1 \mod 19$, $4^{18} \equiv 1 \mod 19$, etc...

6. First note $\left(\frac{5}{31}\right) = (-1)^{2 \cdot 15}\left(\frac{31}{5}\right) = 1 \cdot \left(\frac{1}{5}\right) = 1.$

6. To use GL: We have the interval $(-15.5, 15.5)$, $\frac{31-1}{2} = 15$

and $5, 2\cdot5, 3\cdot5, 4\cdot5, 5\cdot5, 6\cdot5, 7\cdot5, 8\cdot5, 9\cdot5, 10\cdot5, 11\cdot5, 12\cdot5, 13\cdot5, 14\cdot5, 15\cdot5$

$\equiv 5, 10, 15, -11, -6, -1, 4, 9, 14, -12, -7, -2, 3, 8, 13$

mod 31 and in $(-15.5, 15.5)$

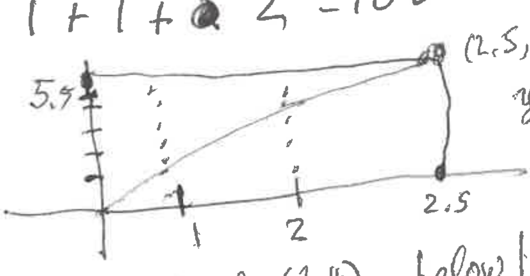
$\#$ neg terms is 6 $\Rightarrow \left(\frac{5}{31}\right) = (-1)^6 = 1$

7. We have to show $\frac{5-1}{2} \cdot \frac{11-1}{2} = \sum_{i=1}^{2}\left[\frac{11 \cdot i}{5}\right] + \sum_{j=1}^{5}\left[\frac{5 \cdot j}{11}\right]$

i.e. $2 \cdot 5 = \left[\frac{11}{5}\right] + \left[\frac{22}{5}\right] + \left[\frac{5}{11}\right] + \left[\frac{10}{11}\right] + \left[\frac{15}{11}\right] + \left[\frac{20}{11}\right] + \left[\frac{25}{11}\right]$

$\parallel$

$10 = 2 + 4 + 0 + 0 + 1 + 1 + 2 = 10$ ✓



$y = \frac{5.5}{2.5}x = 2.2x$

Now the integer points strictly contained in rectangle = 10

(1,1), (1,2), (2,1), (2,2), (2,3), (2,4) below line.

(1,3), (1,4), (1,5) (2,5) above line

(Points in graph not accurate)

(8). write $x = yq + r$.

$$\frac{x}{y} = \frac{8+6i}{3-4i} = (8+6i)\cdot\left(\frac{3+4i}{25}\right)$$

$$= \frac{50i}{25} = 2i$$

$$\Rightarrow x = 2i(3-4i) = 6i+8$$

$$\overset{x}{\underset{8+6i}{\shortparallel}} \Rightarrow y \mid x \Rightarrow GCD(x,y) = y = 3-4i$$