MATH 471 EXAM II ANSWERS

This exam is worth 100 points, with each problem worth 20 points. Please complete Problem 1 and then *any four* of the remaining problems. *There are problems on both sides.* Unless indicated, you must justify your answer to receive credit for a solution.

When submitting your exam, please indicate which problems you want graded by writing them in the upper right corner on the cover of your exam booklet. You must select exactly four problems; any unselected problems will not be graded, and if you select more than four only the first four (in numerical order) will be graded.

(1) Please classify the following statements as *True* or *False*. Write out the word completely; do not simply write T or F. There is no partial credit for this problem, and it is not necessary to show your work for this problem.

Note that for a statement to be *True*, it must be true *exactly as written and for all cases*. To be *False*, there needs to be only one example showing that the statement is false. A statement that is "true most of the time, except sometimes" is false in mathematics.

(a) If $2x \equiv 4 \bmod 8$, then $x \equiv 2, 6 \bmod 8$. **Answer:** True.

(b) Given an integer $N > 1$, using the Pollard ρ-method one can always find a divisor $d \mid N$ with $1 < d < N$. **Answer:** False, what if N is prime?

(c) A two-by-two linear system modulo N either has a unique solution, or N distinct solutions. **Answer:** False, the system can also have no solutions.

(d) Let $m > 1$ be an integer. Let $m = p_1^{e_1} \cdots p_k^{e_k}$ be the prime factorization of m into distinct prime powers. Fix integers a_i for $i = 1, \ldots, k$. Then there is a unique positive integer N such that $N \equiv a_i \bmod p_i^{e_i}$. **Answer:** False, N exists but it is not uniquely determined. Given such an N, we can modify it by adding any multiple of m without changing the congruences mod $p_i^{e_i}$.

(e) Suppose $f(\alpha) \equiv 0 \bmod p$, where p is a prime and $f(x)$ is a polynomial with integer coefficients. Suppose also that α is the only root of f modulo p. Then there are at most p^{r-1} roots of f modulo p^r. **Answer:** True. Think about what can happen when applying Hensel's lemma. When going from any p^{r-1} to p^r, a given root either lifts to a unique root, or to no root, or to p distinct roots. So if there's only one root mod p, there must be at most p^{r-1} roots when we get to p^r. For an example, $f(x) = x^{2^{r-1}} - 1$ has 2^{r-1} roots mod 2^r.

(2) Let $N = 2573$. Use Pollard's ρ method to find a nontrivial divisor of N, using the initial seed $x_0 = 2$ and the function $f(x) = x^2 + 1$. **Answer:** We find that the sequence $\{x_i\}_{i \geq 0}$ mod N is $2, 5, 26, 677, 336, 2258, 1452, \ldots$. The GCDs are $(x_2 - x_1, N) = (x_4 - x_2, N) = 1$ and $(x_6 - x_3, N) = 31$. And $31 \mid N$.

(3) Compute the following modular exponentials. **Answer:** In all these we use the algorithm described in class, which begins by computing the binary expansion of the exponents. Here we just give the answer and the binary expansion of the exponent.

Date: Thursday, 13 November 2008.

(a) $3^{15} \bmod 10$. **Answer:** $15 = 1111_2$, and we get 7.
(b) $3^{512} \bmod 10$. **Answer:** $512 = 1000000000_2$, and we get 1.
(c) $3^{609} \bmod 10$. **Answer:** $609 = 1001100001_2$, and we get 3.

(4) Solve for x:
(a) $2x + 7 \equiv 4 \bmod 17$. **Answer:** $x \equiv -2^{-1} \cdot 3 \equiv 7 \bmod 17$.
(b) $5x + 10 \equiv 11 \bmod 25$. **Answer:** Since $5 \nmid 11$ there are no solutions.
(c) $12x + 4 \equiv 8 \bmod 16$. **Answer:** Divide by 4 to get the conguence $3x + 1 \equiv 2 \bmod 4$. This means $x \equiv 3 \bmod 4$. Going back to modulo 16 we get $x \equiv 3, 7, 11, 15 \bmod 16$.

(5) Use Hensel's lemma to find the roots of the polynomial $f(x) = x^4 + x^3 + x^2 + 1$ modulo $2, 2^2, 2^3, 2^4, 2^5$. **Answer:** The only root mod 2 is $x = 1$, so we lift this. Note that $f'(x) = 4x^3 + 3x^2 + 2x \equiv x^2 \bmod 2$, and $f'(1) \equiv 1 \bmod 2$. This is nonzero, so we always lift to a unique root at each level. We have $-f'(1)^{-1} \equiv 1 \bmod 2$, so we really only have to compute $t \equiv (f(\alpha)/2^e) \bmod 2$ where α is the root mod 2^e, and then the root β mod 2^{e+1} is $\beta = \alpha + 2^e t$. Using this we find the sequence of roots 1 mod 2, 1 mod 4, 5 mod 8, 13 mod 16, 29 mod 32.

(6) Solve the following systems of linear equations:
(a)

$$2x + 3y \equiv 7 \bmod 10$$
$$3x + 4y \equiv 3 \bmod 10$$

Answer: The determinant is $-1 \bmod 10$, so there is a unique solution. If we use Cramer's rule, for instance, we find that $x \equiv (28-9)/(-1) \equiv 1 \bmod 10$ and $y \equiv (6 - 21)/(-1) \equiv 5 \bmod 10$.

(b)

$$3x + 5y \equiv 0 \bmod 7$$
$$x + 4y \equiv 0 \bmod 7$$

Answer: In this one the determinant vanishes mod 7. There is at least one solution, namely $(0, 0)$, so there are actually 7 solutions. If we use the second equation to write $x \equiv 3y \bmod 7$, we get the solutions

$$(0,0), (3,1), (6,2), (2,3), (5,4), (1,5), (4,6).$$

(7) Gus the grocer has many apples. He knows that he has an odd number of apples. When he makes piles of five he has two left over, and when he makes piles of seven he has four left over. He also knows that he has less than 200 apples but more than 100. How many does he have? **Answer:** Use the CRT with the system $x \equiv 1 \bmod 2$, $x \equiv 2 \bmod 5$, $x \equiv 4 \bmod 7$. The first two give $x \equiv 7 \bmod 10$. Then with the third we get $x \equiv 67 \bmod 70$. Since $100 < x < 200$, we have $x = 67 + 70 = 137$.

(8) The set $SL_2(m)$ is the set of all 2×2 matrices modulo m that have determinant $1 \bmod m$.
(a) Find all elements of $SL_2(2)$. (Hint: for $SL_2(p)$ where p is prime there are $(p^2 - 1)(p - 1)$ elements.) **Answer:** There are six elements. The possible top

rows are $x = (1, 0)$, $y = (0, 1)$, and $z = (1, 1)$. For each of these, there are only two choices of bottom row that work, giving 6 total. If we write the choice of two rows as an ordered pair (to save space), we get xy, xz, yx, yz, zx, zy.

(b) How many elements are there in $SL_2(m)$, where $m = 30$? (Hint: CRT) **Answer:** We have $m = 2 \cdot 3 \cdot 5$. Any element of $SL_2(30)$ determines one in each of $SL_2(2), SL_2(3), SL_2(5)$. Conversely, given any element from each of these, we can find a unique one in $SL_2(30)$ using the CRT. So there are $6 \cdot 24 \cdot 120 = 17280$ elements in $SL_2(30)$.

(9) Let $f(x) = x^2 - 1$. Classify all the positive integers m such that $f(x) \equiv 0 \bmod m$ has exactly two distinct solutions. **Answer:** First we consider m a prime power. From class we know that if $m = p^k$ where p is odd, then there are two distinct solutions. Similarly if $m = 2$ there is one solution, if $m = 2^2$ there are two distinct solutions, and if $m = 2^k$, $k \geq 3$ there are four distinct solutions. So if m is a prime power we must have $m = 4$ or $m = p^k$ where p is odd. Now consider more general m and apply the CRT. Write $m = 2^a p_1^{k_1} \cdots p_r^{k_r}$ where all the primes are distinct. If m is odd then it must be a prime power (otherwise if there are more than two odd primes dividing m we'll have at least 4 distinct solutions). If m is even then it must be of the form $2p^k$ or 2^2. Any other even integers will have at least 4 solutions mod m.