MATH 471 EXAM I

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 an integer n has no positive divisor $d \neq 1$ such that $d \leq \sqrt{n}$, then n is prime. **Answer:** True. This is one way to streamline the trial division factorization algorithm. Actually I took either True or False for this since I forgot to say that $n > 0$.

(b) According to the division algorithm, given any integers a, b we can find a unique pair of integers q, r with $0 \leq r < a$ and $b = qa + r$. **Answer:** False. This is almost the statement of the division algorithm (Theorem 1.10 in the text), but we need $a > 0$ for it to be true.

(c) A function f defined on the integers is called *multiplicative* if $f(mn) = f(m)f(n)$ for all integers m, n. **Answer:** False. The integers m, n need to be relatively prime. This is the definition of *strictly* or *fully* multiplicative.

(d) Any two primes are relatively prime to each other. **Answer:** False. The primes must be distinct!

(e) The least common multiple of two integers cannot be computed without first computing their prime factorizations. **Answer:** False. One can use the Euclidean algorithm to compute (a, b), then $[a, b] = (a, b)/ab$.

(2) (a) Compute the prime factorization of 13461525 (you may use any algorithm you like). **Answer:** By inspection we see that 5^2 divides the number. After dividing we see that 3 divides, and in fact 3^3 divides (a number is divisible by 3 iff the sum of its digits is divisible by 3, or just use trial division). This gets us to 19943. Trial division then finds the remaining prime divisors, $7, 11, 37$. The final answer is $3^3 \cdot 5^2 \cdot 7^2 \cdot 11 \cdot 37$.

(b) Use Fermat factorization to find a nontrivial divisor of 1907893 (you don't need to find the full factorization). **Answer:** We have $\lfloor \sqrt{1907893} \rfloor = 1381$, so start

Date: Tuesday, 7 October 2008.

computing $1382^2 - 1907893$, $1383^2 - 1907893$, ... until you hit a perfect square. We hit it right away: $1387^2 - 1907893 = 126^2$. Thus both $1387 - 126 = 1261$ and $1387 + 126 = 1513$ divide our number. Note that these divisors aren't prime. Factoring either one of them with Fermat actually takes a while ...

(3) (a) Compute $(65, 221)$. **Answer:** Pulverize to find 13.
(b) Compute $(65, 221, 93)$. **Answer:** Use $(\alpha, \beta, \gamma) = ((\alpha, \beta), \gamma)$, the output of the first part, and the Pulverizer (or trying to divide 13 into 93) to find $(65, 221, 93) = (13, 93) = 1$.
(c) Find integers a, b such that $65a+221b = (65, 221)$. **Answer:** Use the Extended Euclidean algorithm to get $a = 7, b = -2$. Other answers are possible.
(d) Find integers A, B, C such that $65A + 221B + 93C = (65, 221, 93)$.**Answer:** First use EEA to compute $-6 \cdot 93 + 43 \cdot 13 = 1$. Now substitute $7 \cdot 65 + -2 \cdot 221 = 13$ in for the 13 to get $-6 \cdot 93 + 301 \cdot 65 + -86 \cdot 221 = 1$. Other answers are possible.

(4) For each linear equation, either find all integer solutions, or explain why there are no integer solutions.
(a) $x + y = 1$. **Answer:** Easy by inspection: $x = 1 + k, y = -k, k \in \mathbf{Z}$.
(b) $15x + 12y = 8$. **Answer:** The GCD $(15, 12) = 3$, and $3 \nmid 8$, so no solutions.
(c) $3x + 5y = 10$. **Answer:** The GCD is 1, which divides 10, so infinitely many solutions. A particular solution is $(x, y) = (0, 2)$. Thus all answers are given by $x = 5k, y = 2 - 3k, k \in \mathbf{Z}$. Note that your answer may look different and still be correct.

(5) Let n be a positive integer. Define the *radical* of n, denoted $\mathrm{rad}(n)$, to be the product of the distinct primes dividing n. For example, since $360 = 2^3 \cdot 3^2 \cdot 5$, we have $\mathrm{rad}(n) = 2 \cdot 3 \cdot 5 = 30$.
   (a) Compute $\mathrm{rad}(121)$ and $\mathrm{rad}(968)$. **Answer:** 11 and 22.
   (b) What integers have the property that $\mathrm{rad}(n) = n$? **Answer:** The largest exponent of any prime in the prime factorization must be 1. Such numbers are called *squarefree* because they have no square divisor (other than 1). Prime numbers are squarefree, but there are many numbers that are squarefree that aren't prime.
   (c) Suppose $\mathrm{rad}(mn) = \mathrm{rad}(m)\,\mathrm{rad}(n)$. What can you conclude about m and n? **Answer:** The sets of primes in their prime factorizations must be disjoint, which implies $(m, n) = 1$.
   (d) Can it happen that $\mathrm{rad}(mn) > \mathrm{rad}(m)\,\mathrm{rad}(n)$? Either give an example verifying this, or explain why it can't happen. **Answer:** This can never happen. Consider the prime factorizations of both sides of the inequality. Partition the primes that appear into three sets: S_m, the primes that divide m and not n; S_n, the primes that divide n and not m; and $S_{m,n}$, the primes that divide both m and n. Clearly every prime that appears will appear in one of these sets, and these sets are disjoint. Now the primes in S_m and S_n appear with exponent 1 on both sides, but the primes in $S_{m,n}$ appear with exponent 1 on the left and 2 on the right. Therefore the left must always be $\leq$ the right.
   Here is another argument. (Actually it's basically the same argument, phrased differently.) Consider the prime factorizations of the left and the right. On the left all primes have exponent 1. On the right they all have exponent 1 or 2. If the left is to be bigger than the right, there must be a prime p occuring on the left that doesn't occur on the right (otherwise obviously the right is $\geq$ the left). But if $p \mid mn$ then $p \mid m$ or $p \mid n$. So in fact p must occur on the right, a contradiction.

(6) Let H be the set of positive integers congruent to 1 modulo 4. An integer $h > 1$ in H is called a *Hilbert prime* if h cannot be factored nontrivially into two smaller elements of H. That is, $h \in H$ is a Hilbert prime if and only if for any factorization $h = ab$ with $a, b \in H$, we have $a = h$ or $b = h$.

Note that being a Hilbert prime is not the same as being prime. The first two Hilbert primes are 5 and 9; even though $9 = 3^2$ is not a prime, it cannot be factored into two Hilbert primes, since $3 \notin H$.
   (a) Find all Hilbert primes < 80. **Answer:** List all the numbers that are 1 mod 4 up to 77 and look for the ones that have no divisor appearing earlier in the list. There are 16 altogether: 5, 9, 13, 17, 21, 29, 33, 37, 41, 49, 53, 57, 61, 69, 73, 77.
   (b) Check that $693 \in H$. **Answer:** $693 = 173 \cdot 4 + 1$. This is the only condition to be in H.
   (c) Show that 693 has two different factorizations into Hilbert primes. **Answer:** The prime factorization is $693 = 3^2 \cdot 7 \cdot 11$. So the two factorizations are $21 \cdot 33$ and $9 \cdot 77$. Incidentally, this shows that unique factorization fails for the set H.

(7) Recall from class that $\sigma_k(n)$ is the sum of the kth powers of the divisors of n. For instance, $\sigma_2(10) = 1^2 + 2^2 + 5^2 + 10^2 = 130$.

(a) Compute $\sigma_3(30)$. **Answer:** $1+8+27+125+216+1000+3375+27000 = 31752$.

(b) Let p be a prime. Compute $\sigma_k(p)$ and $\sigma_k(p^r)$. **Answer:** $1 + p^k$ and $1 + p^k + p^{2k} + \cdots + p^{rk}$.

(c) If p is a prime, the function σ_k satisfies the following identity:

$$\sigma_k(p^{r+1}) = \sigma_k(p)\sigma_k(p^r) - p^k\sigma_k(p^{r-1}).$$

Verify the identity for $k = 2$, $p = 2$, and $r = 1, 2, 3$. **Answer:** Just compute it, using the above formulas.

(d) Prove the identity for all p, r and for $k = 0, 1$. (Hint: don't use induction, just compute both sides.) **Answer:** Here is how to prove it for all p, r, k. The left hand side is $1+p^k+p^{2k}+\cdots+p^{rk}+p^{(r+1)k}$. The first product on the right hand side is $1+2p^k+2p^{2k}+\cdots+2p^{rk}+p^{(r+1)k}$, and $-p^k\sigma_k(p^{r-1}) = -p^k-p^{2k}-\cdots-p^{rk}$. Adding these two together we get the left hand side. Incidentally, the function $\sigma_k(m)$ is an example of a multiplicative function that is not fully multiplicative (cf. Problem 1c).