MA 341 Final, due Friday, May 5

You'll be graded on the quality of your writing along with the mathematical content. You are not allowed to discuss these problems with anyone else. Hand in your solutions to the math department office, MCS 142, in my mailbox, by 5 pm on Friday May 5.

1. Prove that if n is odd and not divisible by 3, then $24|n^2 - 1$.

2. Prove that if $a, b \in \mathbf{Z}$ are relatively prime and ab is a perfect cube (that is, the third power of another integer), then a and b are both perfect cubes.

3. Does the Diophantine equation $x^2 - 101y = 14$ have a solution?

4. Find four solutions (x, y, z) to the Diophantine equation $2x^2 + 3y^2 = 5z^2$, where x, y, z are relatively prime positive integers.

5. Find $(1+2i)^{482} \pmod{11}$. Leave your answer in the form $a+bi$, where $0 \leq a, b < 11$.

6. 7001 is prime. How many primitive roots are there modulo 7001?

7. In RSA cryptography, Alice chooses a modulus n and a public key e; she makes n and e available for all to see. When Bob wants to send Alice a secret message m (which is an integer smaller than n and relatively prime to it), he computes $m^e \pmod{n}$ and sends it to Alice. Then Alice can compute m from m^e. Explain why would it be a bad idea to use the modulus $n = 10^{100}$.

8. Let a_1 and a_2 be units modulo m which have orders d_1 and d_2, respectively. (a) Prove that the order of $a_1 a_2$ divides $[d_1, d_2]$. (b) Use a counterexample to show that the order of $a_1 a_2$ is not always equal to $[d_1, d_2]$.

9. Let π be a Gaussian prime whose norm is a prime $p \equiv 1 \pmod 4$. (Example: $\pi = 1 + 2i$, $p = 5$.) Show that for all Gaussian integers α, $\alpha^p \equiv \alpha \pmod \pi$.