18.781 Second Midterm

You can use your book "An Introduction to the Theory of Numbers" and your class notes freely. However, you may not consult any other books or sources. To receive full credit you must justify all your steps.

1. (10 points) Determine the odd primes $p > 5$ for which 15 is a quadratic residue.

2. (15 points) Let p be an odd prime. Show that the numbers

$$1^k, 2^k, \ldots, (p-1)^k$$

form a reduced residue system modulo p if and only if the greatest common divisor of k and $p-1$ is 1.

More generally, let p be an odd prime and let $n > 1$ be an integer. Suppose that $r_1, \ldots, r_{\phi(p^n)}$ forms a reduced residue system modulo p^n. Show that $r_1^k, \ldots, r_{\phi(p^n)}^k$ forms a reduced residue system modulo p^n if and only if the greatest common divisor of k and $p(p-1)$ is 1.

3. (20 points) Prove that there are infinitely many primes of the form $12n+7$. (If you want to receive credit for this problem and you quote Dirichlet's theorem, you have to prove Dirichlet's theorem from scratch. Hint: Show that if x is not divisible by 3, then $4x^2+3$ has a prime factor of the form $12n+7$.)

4. (20 points) Determine with proof the class number of -11. Find the prime numbers that can be represented by a binary quadratic form of discriminant -11.

5. (20 points) Find all the rational solutions of the following equations:
(i) $3x^2 + 5y^2 = 7$
(ii) $x^2 - 7y^2 = 1$

6. (15 points) (i) Using Fermat's descent argument or by any other means show that the only solutions of the equation

$$x^4 - x^2y^2 + y^4 = z^2$$

where x and y are relatively prime occurs when $x^2 = 1, y = 0$ or $x = 0, y^2 = 1$ or $x^2 = y^2 = 1$. (Hint: It might be useful to rewrite the equation as $(x^2-y^2)^2 + x^2y^2 = z^2$.)

Extra credit (ii) (15 points) Using the previous part conclude that four distinct perfect squares cannot form an arithmetic progression. Give an example where three distinct perfect squares do form an arithmetic progression. (Recall that a sequence is an arithmetic progression if the difference between successive terms of the sequence is constant.)