**Number Theory. Final Exam from Spring 2013.**

**Directions:** Provide complete arguments (do not skip steps). State clearly and FULLY any result you are referring to. Partial credit for incorrect solutions, containing steps in the right direction, may be given. If you are unable to solve a problem (or a part of a problem), you may still use its result to solve a later part of the same problem or a later problem in the exam.

**Scoring system:** Exam consists of **6** problems, each of which is worth **12** points. Your regular total is the sum of the best **5** out of **6** scores (so the maximum regular total is 60). If $k$ is the lowest of your 6 scores and $k > 8$, you will get $k - 8$ bonus points (so the maximum total with the bonus is 64).

**1.**

(a) (5 pts) Let $d$ be a positive integer which is not a perfect square. Prove that Pell's equation $x^2 - dy^2 = 1$ has a solution $(x, y)$ with $x > 0$, $y > 0$ and $y$ even.

(b) (7 pts) Find a solution $(x, y)$ to Pell's equation $x^2 - 28y^2 = 1$ with $x > 0$ and $y > 0$. **Hint:** (b) can, of course, be solved by the standard method, but you may use the proof of (a) to solve (b) with very few computations. Solution by guessing is allowed (although direct guessing is not recommended).

**2.** Given a prime $p$ and a nonzero integer $m$, let $ord_p(m)$ denote the largest $e$ such that $p^e \mid m$.

(a) (3 pts) Prove that $ord_p(mn) = ord_p(m) + ord_p(n)$ for any nonzero $m$ and $n$

(b) (2 pts) Give a characterization of perfect squares in terms of $ord_p$ function (for various $p$): a positive integer $n$ is a perfect square if and only if ... (complete the statement, no justification is necessary)

(c) (7 pts) Let $m, n$ and $k$ be positive integers which are coprime as a set (note that $m, n$ and $k$ are not required to be pairwise coprime). Assume that each of the numbers $mn, mk$ and $nk$ is a perfect square. Prove that $m, n$ and $k$ must all be perfect squares. **Hint:** use (a) and (b).

**3.** (12 pts) Let $p \neq 7$ be an odd prime. Compute the Legendre symbol $(\frac{7}{p})$. The final answer should be given in the form

$$\left(\frac{7}{p}\right) = \begin{cases} 1 & \text{if } p \equiv a_1, a_2, \ldots, \text{ or } a_k \mod N \\ -1 & \text{if } p \equiv b_1, b_2, \ldots, \text{ or } b_l \mod N \end{cases}$$

(where $a_1, \ldots, a_k, b_1, \ldots, b_l$ and $N$ are specific integers that you need to determine).

**4.**

(a) (3 pts) State the classification theorem for primitive Pythagorean triples: let $x, y, z \in \mathbb{N}$ with $x$ odd. The following are equivalent:

(i) $x^2 + y^2 = z^2$ and $gcd(x, y, z) = 1$.

(ii) there exist $u, v \in \mathbb{N}$ such that ... (complete the statement).

**Note:** Make sure not to skip any conditions; otherwise, you will have difficulty solving parts (b) and (c).

(b) (5 pts) Given a positive EVEN integer $b$, denote by $n_b$ the number of integer pairs $(x, z)$ such that $x > 0, z > 0$, $gcd(x, b, z) = 1$ and $x^2 + b^2 = z^2$. Prove that $n_b > 0$ if and only if $b$ is divisible by 4.

(c) (4 pts) Find all positive even $b$ for which $n_b = 1$ (and prove your answer).

**5.** Let $R = \mathbb{Z}[\sqrt{3}] = \{a + b\sqrt{3} : a, b \in \mathbb{Z}\}$. Define the function $N : R \to \mathbb{Z}_{\geq 0}$ by $N(a + b\sqrt{3}) = |(a + b\sqrt{3})(a - b\sqrt{3})| = |a^2 - 3b^2|$.

(a) (2 pts) Prove that $N(fg) = N(f)N(g)$ for all $f, g \in R$.

(b) (3 pts) Let $p \in \mathbb{N}$ be a prime, and suppose that there exists no $f \in R$ with $N(f) = p$. Prove that $p$ is irreducible as an element of $R$.

(c) (7 pts) Use (b) to show that if $p \in \mathbb{N}$ is a prime which is congruent to 5 or 7 mod 12, then $p$ is irreducible as an element of $R$.

**Note:** You may use without proof that an element $f \in R$ is a unit if and only if $N(f) = 1$. **Warning:** if you did not use the full power of the assumption on $p$ in (c), your argument is incomplete.

**6.** Given positive integers $m$ and $n > 1$, let $f(n, m)$ be the number of reduced solutions to the congruence

$$x^2 \equiv m \mod n.$$

(a) (9 pts) Assume that $m$ is square-free. Prove that for any odd $n > 1$ either $f(n, m) = 0$ or $f(n, m) = 2^k$ for some integer $k \geq 0$. Clearly state any theorem you are referring to. **Hint:** First reduce to the case when $n$ is a prime power. **Note:** The assertion is actually true for even $n$ as well, but that takes more work to justify.

(b) (3 pts) Give an example (with proof) of a non-square-free integer $m$ for which the assertion of (a) is false for some odd $n$.