Number Theory. Final Exam from Spring 2013. Solutions

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).

Solution: (a) Let (x_0, y_0) be any solution with $x_0 > 0, y_0 > 0$. Then $x_0 + y_0\sqrt{d} \in Pell(d)$ and (since $Pell(d)$ is a group with respect to multiplication) $(x_0 + y_0\sqrt{d})^2 \in Pell(d)$ as well. Since $(x_0 + y_0\sqrt{d})^2 = (x_0^2 + dy_0^2) + 2x_0y_0\sqrt{d}$, the pair $(x, y) = (x_0^2 + dy_0^2, 2x_0y_0)$ is also a solution. It is clear that $x, y > 0$ and y is even.

(b) By direct computation, the continued fraction of $\sqrt{28}$ is $[5; \overline{3, 2, 3, 10}]$. The length of the period is equal to 4 (even), so by the theorem stated in class the numerator and the denominator of the finite continued fraction $[5; 3, 2, 3]$ form a solution to $x^2 - 28y^2 = 1$. We have $[5; 3, 2, 3] = \frac{127}{24}$, so $(127, 24)$ is a solution to $x^2 - 28y^2 = 1$.

Here is a more conceptual solution using (a). Observe that if we found $x_0, y_0 > 0$ with y_0 even such that $x_0^2 - 7y_0^2 = 1$, then $x_0^2 - 28(y_0/2)^2 = 1$, so $(x_0, y_0/2)$ is a solution to $x^2 - 28y^2 = 1$.

One non-trivial solution to $x^2 - 7y^2 = 1$ is easy to guess: $(x, y) = (8, 3)$. To get a solution with y even we use the computation from (a): $(8 + 3\sqrt{7})^2 = 127 + 48\sqrt{7}$. Thus, the pair $(x_0, y_0) = (127, 48)$ satisfies $x_0^2 - 7y_0^2 = 1$, so again we deduce that $(127, 48/2) = (127, 24)$ is a solution to $x^2 - 28y^2 = 1$.

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).

Solution: (a) Let $a = ord_p(m)$ and $b = ord_p(n)$. Then $m = p^a u$ and $n = p^b v$ where $p \nmid u$ and $p \nmid v$. We have $mn = p^{a+b}(uv)$, and $p \nmid uv$ since p is prime. Therefore, $ord_p(mn) = a + b = ord_p(m) + ord_p(n)$.

(b) A positive integer n is a perfect square if and only if $ord_p(n)$ is even for every prime p.

(c) We argue by contradiction. Assume that m is not a perfect square. Then by (b), there is a prime p such that $ord_p(m)$ is odd. Since mn and mk are perfect squares, $ord_p(mn) = ord_p(m) + ord_p(n)$ and $ord_p(mk) = ord_p(m) + ord_p(k)$ must be even. Since $ord_p(m)$ is odd, we conclude that $ord_p(n)$ and $ord_p(k)$ are also odd. In particular, all three numbers $ord_p(m)$, $ord_p(k)$ and $ord_p(n)$ are nonzero, so p divides m, n and k. This contradicts the assumption that m, n and k are coprime as set.

Thus, we proved that m is a perfect square. Analogous argument shows that n and k must be perfect squares as well.

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).

Solution: By Problem 3(b) from the second midterm,

$(\frac{7}{p}) = 1 \iff (p \equiv 1 \mod 4 \text{ and } (\frac{p}{7}) = 1)$ or $(p \equiv 3 \mod 4 \text{ and } (\frac{p}{7}) = -1)$.

By direct computation, $(\frac{p}{7}) = 1$ if $p \equiv 1, 2, 4 \mod 7$ and $(\frac{p}{7}) = -1$ if $p \equiv 3, 5, 6 \mod 7$. Note that

- $(p \equiv 1 \mod 4 \text{ and } p \equiv 1 \mod 7) \iff p \equiv 1 \mod 28$
- $(p \equiv 1 \mod 4 \text{ and } p \equiv 2 \mod 7) \iff p \equiv 9 \mod 28$
- $(p \equiv 1 \mod 4 \text{ and } p \equiv 4 \mod 7) \iff p \equiv 25 \mod 28$
- $(p \equiv 3 \mod 4 \text{ and } p \equiv 3 \mod 7) \iff p \equiv 3 \mod 28$
- $(p \equiv 19 \mod 4 \text{ and } p \equiv 5 \mod 7) \iff p \equiv 19 \mod 28$
- $(p \equiv 3 \mod 4 \text{ and } p \equiv 6 \mod 7) \iff p \equiv 27 \mod 28$

Thus,

$$\left(\frac{7}{p}\right) = 1 \iff p \equiv 1, 3, 9, 19, 25, 27 \mod 28.$$

There are 12 integers in $[1, 28]$ which are coprime to 28:

$$1, 3, 5, 9, 11, 13, 15, 17, 19, 23, 25, 27.$$

Therefore,

$$\left(\frac{7}{p}\right) = -1 \iff p \equiv 5, 11, 13, 15, 17, 23 \mod 28.$$

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).

Solution: (a) (ii) there exist $u, v \in \mathbb{N}$ such that $u > v$, u and v have different parity, $x = u^2 - v^2$ and $y = 2uv$.

(b) By classification of primitive Pythagorean triples, $n_b > 0$ if and only if b can be written as $2uv$ where u and v have different parity. Clearly, if $4 \nmid b$, there are no such u and v (since either u or v must be even, so 4 must divide $2uv$). On the other hand, if $4 \mid b$, we write $b = 2^e c$ with $e \geq 2$ and c odd. Then we can set $u = 2^{e-1}$ and $v = c$ if $2^{e-1} > c$ and $u = c$ and $v = 2^{e-1}$ if $2^{e-1} < c$.

(c) By the same argument as in (b), $n_b = 1 \iff b$ can be UNIQUELY written as $2uv$ where u and v have different parity and $u > v$. We claim that this happens $\iff b = 2^e$ for some $e \geq 2$ (that is, b is a power of 2 greater than or equal to 4).

Indeed, if $b = 2^e$ and $b = 2uv$, then both u and v are powers of 2 (possibly the zero power $2^0 = 1$), so the only way for u and v to have different parity and satisfy $u > v$ is to set $u = 2^{e-1}$ and $b = 1$.

Suppose now that b is not a power of 2. Then b has an odd prime divisor p. If $4 \nmid b$, then $n_b = 0$ by (b). If $4 \mid b$, we can write $b = 2uv$ in two different ways:

(i) $u = b/2$ and $v = 1$
(ii) ($u = b/(2p)$ and $v = p$) if $b/(2p) > p$ and ($u = p$ and $v = b/(2p)$) if $b/(2p) < p$.

In both case $u > v$ and u and v have different parity.

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.

Solution: (a) A conceptual way to prove this equality is described in Problem 2 of HW#9. Here we present a solution by brute force: suppose that $f = a + b\sqrt{3}$ and $g = c + d\sqrt{3}$. Then $fg = (ac + 3bd) + (ad + bc)\sqrt{3}$, so $N(f)N(g) = |a^2 - 3b^2| \cdot |c^2 - 3d^2| = |a^2c^2 - 3a^2d^2 - 3b^2c^2 + 9b^2d^2|$ while

$$\begin{aligned} N(fg) = |(ac+3bd)^2 - 3(ad+bc)^2| &= |a^2c^2 + 6acbd + 9b^2d^2 - 3a^2d^2 - 3b^2c^2 - 6adbc| \\ &= |a^2c^2 + 9b^2d^2 - 3a^2d^2 - 3b^2c^2|. \end{aligned}$$

Therefore, $N(f)N(g) = N(fg)$.

(b) Suppose that p is not irreducible as an element of R. Clearly, p is nonzero and not a unit in R (since $\frac{1}{p} \notin R$), so the only possibility is that p is a product of two non-units: $p = fg$. Taking norms of both sides, we get $p^2 = N(fg) = N(f)N(g)$. Since f and g are non-units, both $N(f)$ and $N(g)$ are greater than 1. Hence the only possibility is that $N(f) = N(g) = p$ which is impossible by assumption.

(c) By (b) we need to show that if $p \equiv 5$ or 7 mod 12, then the equation $|a^2 - 3b^2| = p$ has no integer solutions in a and b. Suppose, on the contrary, that such a and b exist. Then $a^2 - 3b^2 = \pm p$, so in either case $a^2 - 3b^2 \equiv \pm 5 \mod 12$ (since $7 \equiv -5 \mod 12$ and $-7 \equiv 5 \mod 12$).

Case 1: $a^2 - 3b^2 \equiv 5 \mod 12$. Then $a^2 - 3b^2 \equiv 5 \mod 3$, whence $a^2 \equiv 2 \mod 3$, and we know that this is impossible.

Case 2: $a^2 - 3b^2 \equiv -5 \mod 12$. Then $a^2 - 3b^2 \equiv -5 \mod 4$, whence $a^2 + b^2 \equiv -5 \equiv 3 \mod 4$. Again this is impossible since $x^2 \equiv 0$ or 1 mod 4 for all $x \in \mathbb{Z}$.

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.

Solution: (a) By the general theory of polynomial congruences we know that if $p_1^{a_1} \dots p_t^{a_t}$ is the prime factorization of n, then $f(n, m) = \prod_{i=1}^{t} f(p_i^{a_i}, m)$. If we show that each $f(p_i^{a_i}, m)$ is 0 or a power of 2, then the same is true for $f(n, m)$. Thus, it is sufficient to consider the case where n is a prime power.

Let us start with the subcase when n itself is prime. Then, since $x^2 - m$ is a quadratic polynomial which has a coefficient not divisible by n, we know that $x^2 \equiv m \mod n$ has 0, 1 or 2 reduced solutions.

Now suppose that $n = p^a$ where p is prime and $a \geq 2$. Let $f(x) = x^2 - m$.

Subcase 1: $p \mid m$. We claim that the congruence $f(x) \equiv 0 \mod n$ has no solution. Indeed, if $x^2 - m \equiv 0 \mod p^a$ for some x, then $x^2 - m = p^a l$ for some $l \in \mathbb{Z}$, so (since $p \mid m$), p must divide x as well. But then $m = x^2 - p^a l$ is divisible by p^2, which contradicts the assumption that m is square-free.

Subcase 2: $p \nmid m$. Let x_0 be any reduced solution to the congruence $f(x) \equiv 0 \mod p$ (as we just showed there are 0, 1 or 2 choices for x_0). Then $p \nmid x_0$ (for any choice of x_0). Note that $f'(x_0) = 2x_0$. Since p is odd, $p \nmid 2$, whence $f'(x_0) \not\equiv 0 \mod p$, so by the lifting theorem, x_0 lifts to unique reduced solution to $f(x) \equiv 0 \mod n$. It follows that $f(x) \equiv 0 \mod n$ has 0, 1 or 2 reduced solutions (and we are done).

(b) Let $m = 9$ and $n = 27$. Then the congruence $x^2 - m \equiv 0 \mod n$ has 6 reduced solutions $x = 3, 6, 12, 15, 21, 24$.