Number Theory, Fall 2016. Solutions to Test #4.

1. In all parts of this problem make sure to include all the calculations.

(a) (4 pts) Find a non-trivial solution to the equation $x^2 - 23y^2 = 1$

(b) (4 pts) Find a non-trivial solution to the equation $x^2 - 53y^2 = 1$

(c) (2 pts) Let $k \in \mathbb{N}$. Compute the continued fraction $[k; k, k, k, \ldots]$

Solution: (a) The continued fraction for $\sqrt{23}$ is $[4; \overline{1, 3, 1, 8}]$. It has even period 4, so the continued fraction $[4; 1, 3, 1]$ gives us a solution. We have $[4; 1, 3, 1] = [4; 1, 4] = [4; 5/4] = 24/5$, so $(24, 5)$ is a solution.

(b) The continued fraction for $\sqrt{53}$ is $[7; \overline{3, 1, 1, 3, 14}]$. It has odd period 5, so the continued fraction $[7; 3, 1, 1, 1]$ give us an element of $\mathbb{Z}[\sqrt{53}]$ of norm -1. We have $[7; 3, 1, 1, 3] = [7; 3, 1, 4/3] = [7; 3, 7/4] = [7; 25/7] = 182/25$, so $N(182 + 25\sqrt{53}) = -1$ and therefore $N((182 + 25\sqrt{53})^2) = 1$. Since $(182 + 25\sqrt{53})^2 = (182^2 + 25^2 \cdot 53 + 50 \cdot 182\sqrt{53}) = 66249 + 9100\sqrt{53}$, the pair $(66249, 9100)$ is a solution.

2. (10 pts) In all parts of this problem by a solution we mean an integer solution

(a) Let $d, c \in \mathbb{Z}$ where $d > 0$ and d is not a perfect square. Prove that if the equation $x^2 - dy^2 = c$ has a solution, then it has infinitely many solutions.

(b) Let p be a prime such that $p \equiv 3 \mod 4$. Prove that the equation $x^2 - py^2 = p$ has no solutions.

(c) Assume that $d \in \mathbb{N}$ is not a perfect square and that the continued fraction for $\sqrt{d}$ has **odd** period. Prove that $x^2 - dy^2 = d$ has a solution.

Solution: (a) This part should have had an extra hypothesis $c \neq 0$ (otherwise the statement is false). So assume that $c \neq 0$ and there exist $a, b \in \mathbb{Z}$ such that $a^2 - db^2 = c$. Thus, if $y = a + b\sqrt{d}$, then $N(y) = c$ (note that $y \neq 0$ since $c \neq 0$).

Since $d > 0$ is not a perfect square, the set $Pell(d) = \{z \in \mathbb{Z}[\sqrt{d}] : N(z) = 1\}$ is infinite. For any $z \in Pell(d)$ we have $N(zy) = N(z)N(y) =$

$1 \cdot c = c$. If $z_1 \neq z_2$, then $z_1 y \neq z_2 y$ (since $y \neq 0$), so there are infinitely many elements of norm c in $\mathbb{Z}[\sqrt{d}]$ and thus infinitely many solutions to the equation $x^2 - dy^2 = c$.

(b) Since $p \equiv 3 \equiv -1 \mod 4$, we have $x^2 - py^2 \equiv (x^2 - (-y^2)) = x^2 + y^2 \mod 4$. Since $x^2, y^2 \equiv 0$ or $1 \mod 4$, we have $x^2 + y^2 \equiv 0, 1, 2 \mod 4$, so $x^2 + y^2 \not\equiv p \mod 4$.

(c) Since the continued fraction for $\sqrt{d}$ has odd period, we know that there exist $a, b \in \mathbb{Z}$ such that $a^2 - db^2 = -1$. Multiplying both sides by $-d$, we get $(db)^2 - da^2 = d$, so the pair (db, a) is a solution to $x^2 - dy^2 = d$.

3. (10 pts) Find all primitive integer solutions to the equation $x^2 + 3y^2 = z^2$ (as usual (x, y, z) is primitive if $gcd(x, y, z) = 1$).

We claim that every primitive solution has the form (a) or (b) below and all primitive solutions can be obtained in this way.

(a) $(x, y, z) = (\pm(3u^2 - v^2), \pm 2uv, \pm(3u^2 + v^2))$ where $u, v \in \mathbb{Z}$ are coprime, have different parity and $3 \nmid v$ (the signs for x, y and z are chosen independently)

(b) $(x, y, z) = (\pm\frac{3u^2 - v^2}{2}, \pm uv, \pm\frac{3u^2 + v^2}{2})$ where $u, v \in \mathbb{Z}$ are coprime, both odd and $3 \nmid v$.

Part I: First we will show that each of the triples in (a) and (b) is a primitive solution. By direct verification we see that each (x, y, z) of the form (a) or (b) satisfies the equation $x^2 + 3y^2 = z^2$. Note that in case (b) the assumption that u and v are both odd ensures that $x, y, z \in \mathbb{Z}$. Now let us prove that all such triples are primitive.

Suppose, by way of contradiction, that there exists a prime p that divides $\pm(3u^2 - v^2), \pm 2uv$ and $\pm(3u^2 + v^2)$ where u, v are as in (a). Then $p \mid 6u^2 = (3u^2 - v^2 + 3u^2 + v^2)$ and $p \mid 2v^2 = (3u^2 + v^2 - (3u^2 - v^2))$. Since $3 \nmid v$, it follows from $p \mid 2v^2$ that $p \neq 3$, hence $p \mid 6u^2$ implies $p \mid 2u^2$. Thus, p divides $2u^2$ and $2v^2$, so $p \mid gcd(2u^2, 2v^2) = 2gcd(u, v)^2 = 2$, so $p = 2$. But u and v have different parity, so $3u^2 - v^2$ is odd and hence $2 \nmid 3u^2 - v^2$, a contradiction.

Similarly, we argue that each triple in (b) is primitive – if we assume that some prime p divides all three numbers x, y, z in (b), arguing as in the previous paragraph, we get $p \mid gcd(u^2, v^2) = gcd(u, v)^2 = 1$, a contradiction.

Part II: Now we will show that each primitive solution comes from (a) or (b) above. First note that there are no primitive solutions with $z = 0$ or $x = 0$, and the only primitive solutions with $y = 0$ are $(\pm 1, 0, \pm 1)$, which come from (a) with $u = 0$ and $v = 1$. Thus, it suffices to find all primitive solutions with x, y, z nonzero; moreover, since each of the sets (a) and (b) is invariant under the sign change in each coordinate, it is enough to find primitive solutions (x, y, z) with x, y, z positive. Clearly, we must have $x < z$ for each such solution.

So, let (x, y, z) be a primitive solution with $x, y, z > 0$. First we claim that $gcd(x, z) = 1$. If not, then there is a prime p which divides both x and z. But then p^2 divides $z^2 - x^2 = 3y^2$ which forces $p \mid y$, in which case (x, y, z) is not primitive. Since $gcd(x, z) = 1$, by a HW#1 problem we must have $gcd(z - x, z + x) = 1$ or 2.

Next we note that x must be odd. Indeed, if x is even, then y and z are both odd (in which case $x^2 + 3y^2 \equiv 3 \mod 4$ while $z^2 \equiv 1 \mod 4$) or y and z are both even (in which case (x, y, z) is not primitive).

Since x is odd, exactly one of y and z is odd, and we consider two cases accordingly.

Case 1: z is even, y is odd. Rewrite our equation as

$$3y^2 = (z - x)(z + x). \tag{$***$}$$

We know that $gcd(z - x, z + x) = 1$ or 2; moreover $z - x$ and $z + x$ are both odd, so we must have $gcd(z - x, z + x) = 1$. From (***) we get that exactly one of the numbers $z - x$ and $z + x$ is divisible by 3.

Subcase 1: $3 \mid (z-x)$. Then we can rewrite (***) as $y^2 = \frac{z-x}{3}(z+x)$, with both factors on the right-hand side still integers. Since $gcd(z-x, z+x) = 1$, we clearly have $gcd(\frac{z-x}{3}, z + x)$ as well. Moreover, $\frac{z-x}{3}$ and $z + x$ are both positive. A product of two coprime positive integers is a perfect square if and only if each of them is a perfect square, so there exist $u, v \in \mathbb{N}$ such that $\frac{z-x}{3} = u^2$ and $z + x = v^2$, and (***) yields $y^2 = u^2v^2$, whence $y = uv$ (since $y > 0$). Solving $\frac{z-x}{3} = u^2$ and $z + x = v^2$ for x and z, we get $z = \frac{3u^2+v^2}{2}$ and $x = \frac{3u^2-v^2}{2}$. Clearly, we must have $gcd(u, v) = 1$ and $3 \nmid v$, for otherwise (x, y, z) is not primitive. Also u and v must have the same parity for x to be an integer, and since u and v are coprime, they must both be odd. Thus (x, y, z) is of the form described in (b).

Subcase 2: $3 \mid (z + x)$. Then we can rewrite (***) as $y^2 = (z - x)\frac{z+x}{3}$, with both factors on the right-hand side still integers. Arguing similarly to subcase 1, we conclude that there exist $u, v \in \mathbb{N}$ such that $x = \frac{v^2-3u^2}{2} = -\frac{3u^2-v^2}{2}$, $y = uv$ and $z = \frac{3u^2+v^2}{2}$, and then deduce (by the same argument) that u, v must satisfy the restrictions from (b).

Case 2: z is odd, y is even. In this case $y, z - x$ and $z + x$ all even, so we can rewrite our equation as

$$3\left(\frac{y}{2}\right)^2 = \frac{z - x}{2} \cdot \frac{z + x}{2},$$

with all factors above being integers. This time $gcd(z - x, z + x) = 2$, so $gcd(\frac{z-x}{2}, \frac{z+x}{2}) = 1$. Again 3 divides exactly one of the numbers $\frac{z-x}{2}$ and $\frac{z+x}{2}$, so splitting into two subcases and arguing similarly to Case 1, we conclude that (x, y, z) must be of the form described in (a).

4. (10 pts) Let Λ be the set of all completely multiplicative functions from $\mathbb{N}$ to $\mathbb{C}$, and let Δ be the set of all multiplicative functions $f : \mathbb{N} \to \mathbb{C}$ with the property that $f(n) = 0$ whenever n is not square-free. Recall that according to our definition, a multiplicative (or completely multiplicative) function g must satisfy $g(1) = 1$

(a) Let $h \in \Lambda$, and let $H = h^{-1}$, the Dirichlet inverse of h. Prove that $H(n) = h(n)\mu(n)$ for all n and deduce that $H \in \Delta$ (here $h(n)\mu(n)$ is the regular multiplication).

(b) Now prove that for any $f \in \Delta$, its Dirichlet inverse lies in Λ.

(c) Recall that the set M of all multiplicative functions forms a group with respect to the Dirichlet product. Note that parts (a) and (b) simply say that $\Lambda = \Delta^{-1}$, that is, Λ is precisely the set of inverses of elements of Δ (and vice versa). Now let $\langle \Delta \rangle_+$ be the set of elements of M representable as $f_1 * \ldots * f_k$ with each $f_i \in \Delta$ and $k \geq 1$ (in group-theoretic terminology, $\langle \Delta \rangle_+$ is the semigroup generated by Δ). Prove that the intersection $\langle \Delta \rangle_+ \cap \Lambda$ contains just 1 element, the function I. **Hint:** What can you say about the values of elements of $\langle \Delta \rangle_+$ and Λ on prime powers?

Solution: (a) It is more convenient to switch how H is defined and what we have to prove about it, that is, we will redefine H by the formula $H(n) = h(n)\mu(n)$ and show that, defined in this way, H is the Dirichlet inverse of h, that is $H * h = I$. We have

$$(H * h)(n) = \sum_{d|n} h(d)\mu(d)h(n/d) = \sum_{d|n} \mu(d)h(n) = h(n) \sum_{d|n} \mu(d),$$

where the second equality holds by complete multiplicativity of h.

Since by definition μ is the Dirichlet inverse of the function u defined by $u(n) = 1$ for all n, we have $\sum_{d|n} \mu(d) = \sum_{d|n} \mu(d)u(n/d) = (\mu * u)(n) = I(n)$. Thus, $(H * h)(1) = h(1)I(1) = 1$ and $(H * h)(n) = h(n)I(n) = 0$ for $n > 1$, so $H * h = I$, as desired.

The other assertions of (a) are now clear – H is multiplicative since $H = h^{-1}$ and we proved in class that multiplicative functions form a group (alternatively, it is clear that the pointwise product of two multiplicative functions is multiplicative, and by definition H is the pointwise product of h and μ). Also, $H(n) = 0$ whenever n is not square-free since μ has the same property. Thus, by definition $H \in \Delta$.

(b) Since f is multiplicative, f^{-1} is also multiplicative. It is easy to see that a multiplicative function g is completely multiplicative if and only if $g(p^a) = g(p)^a$ for every prime p and integer $a \geq 1$. Thus, we just need to check that f^{-1} has the latter property.

For $a \geq 1$ and a prime p we have $(f^{-1} * f)(p^a) = I(p^a) = 0$; on the other hand, by definition,

$$(f^{-1} * f)(p^a) = \sum_{b=0}^{a} f^{-1}(p^b) f(p^{a-b}) =$$
$$f^{-1}(p^{a-1})f(p) + f^{-1}(p^a)f(1) = f^{-1}(p^{a-1})f(p) + f^{-1}(p^a),$$

where the second equality holds since $f \in \Delta$.

Therefore, $f^{-1}(p^a) = -f^{-1}(p^{a-1})f(p)$. We also know that $f^{-1}(1) = 1$ (since f^{-1} is multiplicative). From these equalities by straightforward induction we get

$$f^{-1}(p^a) = (-1)^a f(p)^a \text{ for all } a \geq 1.$$

In particular, $f^{-1}(p^a) = (-f(p))^a = (f^{-1}(p))^a$, as desired.

(c) Clearly, $I \in \langle \Delta \rangle_+ \cap \Lambda$. Conversely, take any $f \in \langle \Delta \rangle_+ \cap \Lambda$, that is, f is completely multiplicative and $f = f_1 * \ldots * f_k$ for some $f_1, \ldots, f_k \in \Delta$. By straightforward induction on k we get the following formula for the Dirichlet product of k functions:

$$f(n) = (f_1 * \ldots * f_k)(n) = \sum_{n = d_1 \ldots d_k} f_1(d_1) \ldots f_k(d_k).$$

Now let $n = p^{k+1}$ for some prime p. We get

$$f(p^{k+1}) = \sum_{e_1 + \ldots + e_k = k+1} f_1(p^{e_1}) \ldots f_k(p^{e_k}).$$

For each term in the above sum, at least one of the e_i's is ≥ 2, and therefore $f_i(p^{e_i}) = 0$ (as $f_i \in \Delta$). Thus, each term (and hence the entire sum) is equal to 0.

Thus, $f(p^{k+1}) = 0$. Since f is completely multiplicative, $f(p^{k+1}) = f(p)^{k+1}$, so $f(p) = 0$ for each prime p. Therefore, again since f is completely multiplicative, for any $n > 1$ we have $f(n) = f(p_1^{a_1} \ldots p_k^{a_k}) = f(p_1)^{a_1} \ldots f(p_k)^{a_k} = 0$. Therefore, $f = I$.