Problem of the Week 9, Spring 2006

Solution by the organizers (Based on Euler's original proof 1738) . We will prove that the only rational solutions to the equation $m^2 - n^3 = 1$ are $(m,n) = (-1,0),(1,0),(0,-1),(3,2),(-3,2)$. If $n = 0$ then $m = \pm 1$ are all possible solutions, similarly if $m = 0$ then $n = -1$ is the only solution. Suppose $n, m \neq 0$ and $n = a/b$ with $a, b \in \mathbb{Z}$, $b > 0$, and $\gcd(a,b) = 1$. Then

$$m^2 b^4 = a^3 b + b^4, \tag{1}$$

that is $b\left(a^3 + b^3\right) = b\,(a+b)\left(a^2 - ab + b^2\right)$ is a non-zero square. Let $c = a + b$, then equation (1) becomes

$$m^2 b^4 = bc\left(3b^2 - 3bc + c^2\right). \tag{2}$$

If $c = 3b$ then $a = 2b$ and $n = 2$ which gives the solutions $m = \pm 3$. From now on assume $c \neq 3b$. Notice that $\gcd(b,c) = \gcd(b, a+b) = \gcd(b,a) = 1$ and $\gcd(3b^2 - 3bc + c^2, b) = \gcd(c^2, b) = 1$. Assume that the pair (b,c) satisfies that $|b|$ is as small as possible such that the right-hand side of (2) is a square. We will show that, once $c = 3b$ is excluded, there are no other solutions by the method of infinite descent. That is we will find a new pair (b', c') with $|b'| < b$. To do this we first divide in two cases.

Case 1 3 *does not divide* c.

Then $\gcd(3b^2 - 3bc + c^2, c) = \gcd(3b^2, c) = \gcd(b^2, c) = 1$. Thus in equation (2) we have the product of three integers pairwise coprime which equals a square. Additionally $b > 0$ and $3b^2 - 3bc + c^2 \geq 3(b - c/2)^2 \geq 0$. Thus each of b, c, and $3b^2 - 3bc + c^2$ are squares. Then there are positive integers p and q such that $\gcd(p,q) = 1$ and

$$\begin{aligned} 3b^2 - 3bc + c^2 &= \left(b\frac{p}{q} - c\right)^2 \\ &= \frac{b^2p^2}{q^2} - \frac{2bpq}{q} + c^2. \end{aligned}$$

Thus

$$\frac{b}{c} = \frac{3q^2 - 2pq}{3q^2 - p^2}. \tag{3}$$

Now we divide in two subcases.

Case1.1. 3 does not divide p.

Suppose P is a prime common divisor of $3q^2 - 2pq$ and $3q^2 - p^2$. Then either $P|q$ or $P|(3q - 2p)$. If $P|q$ then $P|p^2$ which is a contradiction since $\gcd(p,q) = 1$. Thus $P|(3q - 2p)$ on the other hand $P|\left(3q^2 - 2pq\right) - \left(3q^2 - p^2\right) = p^2 - 2pq$. Thus either $P|p$ or $P|(p - 2q)$. If $P|p$ then $P|3q^2$ but $P \neq 3$ (since 3 does not divide p), so $P|q^2$ which is a contradiction. Therefore we must have that $P|(p - 2q)$. Thus $P|\left(3q - 2p\right) + 2\left(p - 2q\right) = -q$ which is a case we considered before. Therefore our conclusion is that $\gcd(3q^2 - 2pq, 3q^2 - p^2) = 1$.

This implies that $b = 3q^2 - 2pq$ and $c = 3q^2 - p^2$ or $b = 2pq - 3q^2$ and $c = p^2 - 3q^2$. However since c is a square we must have $c \equiv 0, 1 \pmod 4$ and $3q^2 - p^2 \equiv 3, 2 \pmod 4$ since we cannot have both p and q even. Therefore the first option is discarded and we have that

$$b = 2pq - 3q^2 \text{ and } c = p^2 - 3q^2.$$

Now recall that c is a square, so there are positive integers r, s with $\gcd(r, s) = 1$ such that

$$\begin{aligned} p^2 - 3q^2 &= \left(p - \frac{r}{s}q\right)^2 \\ &= p^2 - \frac{2pqr}{s} + \frac{r^2q^2}{s^2}. \end{aligned}$$

This implies that

$$\frac{p}{q} = \frac{r^2 + 3s^2}{2rs}$$

and

$$\frac{b}{q^2} = \frac{2p}{q} - 3 = \frac{3s^2 - 3rs + r^2}{rs},$$

which means that

$$\frac{r^2s^2b}{q^2} = rs\left(3s^2 - 3rs + r^2\right)$$

and the left-hand side of the equation is a square since b is a square, thus we obtained an equation of the same form as (2) but $0 < s < b$ which we will check later.

Case1.2. 3 divides p.

Let $p = 3P$ then equation (3) becomes

$$\frac{b}{c} = \frac{q^2 - 2Pq}{q^2 - 3P^2}.$$

By an argument similar to the previous case we can check that $\gcd(q^2 - 2Pq, q^2 - 3P^2) = 1$. And again similarly to last case $3P^2 - q^2$ cannot be a square because it fails modulo 4. Therefore we must have

$$q^2 - 3P^2 = c \text{ and } q^2 - 2Pq = b.$$

But c is a square, so there are positive integers r, s such that

$$\begin{aligned} q^2 - 3P^2 &= \left(q - \frac{r}{s}P\right)^2 \\ &= q^2 - \frac{2qrP}{s} + \frac{r^2P^2}{s^2}. \end{aligned}$$

This implies that

$$\frac{2P}{q} = \frac{4sr}{3s^2 + r^2}$$

and

$$\frac{b}{q^2} = 1 - \frac{2P}{q} = \frac{3s^2 - 4sr + r^2}{3s^2 + r^2} = \frac{(3s - r)(s - r)}{3s^2 + r^2}.$$

Then

$$\frac{b\left(3s^2 + r^2\right)^2}{q^2} = \left(3s^2 + r^2\right)(3s - r)(s - r).$$

Note that the left hand side is a square since b is a square, and if we let $t = s - r$ and $u = 3s - r$ then the right hand side becomes

$$tu\left(3t^2 - 3ut + u^2\right).$$

Similarly to last case we also have that $0 < t < b$ (To be checked later).

Case 2 3 *divides* c.

Let $c = 3C$. Then $\gcd(3C, b) = 1$ and equation (2) becomes

$$\frac{m^2 b^4}{9} = bC\left(b^2 - 3bC + 3C^2\right).$$

Moreover $\gcd(b^2 - 3bC + 3C^2, b) = \gcd(3C^2, b) = \gcd(C^2, b) = 1$, and $\gcd(b^2 - 3bC + 3C^2, C) = \gcd(b^2, C) = 1$. Thus b, C, and $b^2 - 3bC + 3C^2$ are all squares and then we can apply Case 1 from here.

In each of the three cases we obtain an expression like the right hand side of equation (2) which is equal to a square, however in each case we contradict the minimality of the solution. Therefore there are no other solutions.

Now we go over the technical aspects of proving that $0 < s < b$ in Case 1.1 and $0 < t < b$ in Case 1.2.

Claim 3 *In Case 1.1 we have that* $0 < s < b$.
Proof. *First note that* $b = q(2p - 3q)$ *so we have that* $0 < q \leq b$. *Also we know that* $q/p = 2rs/\left(r^2 + 3s^2\right)$. *Now note that* $\gcd\left(s, r^2 + 3s^2\right) = \gcd\left(s, r^2\right) = 1$ *and* $\gcd\left(r, r^2 + 3s^2\right) = \gcd\left(r, 3s^2\right) = \gcd(r, 3)$. *Therefore* $2rs$ *and* $r^2 + 3s^2$ *have a greatest common factor of* $1, 2, 3$ *or* 6. *So if* $3 \nmid r$ *then the greatest common factor is 2, thus* $q = rs$ *or* $q = 2rs$ *and consequently* $s \leq q$. *On the other hand if* $3|r$ *then the greatest common factor is* 3 *or* 6. *Thus* $q = rs/3$ *or* $2rs/3$ *and consequently* $rs/3 \leq q$. *However* $3 \leq r$, *thus* $s \leq q$. *In any case we conclude that* $0 < s \leq q \leq b$.

Equality occurs if $b = q$ *which implies that* $2p - 3q = 1$ *and then*

$$\begin{aligned} 4c &= 4\left(p^2 - 3q^2\right) = (2p)^2 - 12q^2 \\ &= (1 + 3q)^2 - 12q^2 = 1 + 6q - 3q^2 \\ &= 1 + 6b - 3b^2. \end{aligned}$$

But c *is a square, thus* $6b - 3b^2 + 1 = 3b(2 - b) + 1 > 0$. *But if* $b > 2$ *then* $3b(2 - b) < -6$. *Also if* $b = 2$ *then* $1 = 2p - 3b = 2p - 6$ *which is impossible by parity; and finally if* $b = 1$ *then* $c = 1$ *which gives* $a = 0$ *that was excluded to begin with.* ■

Claim 4 *In Case 1.2 we have that* $0 < |t| < b$.

Proof. Similarly to last case $b = q(q - 2P)$, so $0 < q \leq b$. Also $P/q = 2sr/(3s^2 + r^2)$ and again $\gcd(2sr, 3s^2 + r^2)$ is either $1, 2, 3$, or 6. In all cases we can deduce that $q \geq (3s^2 + r^2)/6$. We have that $s = (u - t)/2$ and $r = (u - 3t)/2$ thus

$$\begin{aligned} q &\geq \frac{1}{6}\left(3\left(\frac{u-t}{2}\right)^2 + \left(\frac{u-3t}{2}\right)^2\right) \quad (4) \\ &\geq \frac{1}{4}\left(u^2 - 4ut + 5t^2\right) \\ &\geq \frac{1}{4}\left((u-2t)^2 + t^2\right). \end{aligned}$$

If $|t| \geq 4$ then $t^2 \geq 4|t|$ and consequently $q \geq |t| > 0$. If $|t| = 3$ and $(u - 2t) \neq 0$ then $(u - 2t)^2 + t^2 \geq 10$ and then $q \geq 3 = |t|$. Otherwise $u - 2t = 0$ and $s = 3t/2$ which is not an integer. If $|t| = 2$ and $|u - 2t| \geq 2$ then $(u - 2t)^2 + t^2 \geq 8$ and thus $q \geq |t|$. The other possibilities are as follows, if $u - 2t = 0$ then $r = -t/2$ and $s = 3t/2$ which is impossible since both must be positive. If $u - 2t = \pm 1$ then $s = (t \pm 1)/2$ which is not an integer. If $|t| = 1$ then since q is an integer we must have $q \geq 1 = |t|$. Finally, if $t = 0$ then $s = r = u/2$ which implies that $P = 1, q = 2$, and $b = 0$ which is impossible.

In all possibilities we obtain $q \geq |t| > 0$, with equality if $b = q$ which implies that $b - 2P = q - 2P = 1$ and then

$$\begin{aligned} c &= q^2 - 3P^2 = b^2 - 3\left(\frac{b-1}{2}\right)^2 \\ &= \frac{(b+3)^2 - 12}{4}. \end{aligned}$$

But c is a square, say $c = C^2$, then the last equation becomes $12 = (b+3)^2 - (2C)^2 = (b + 3 + 2C)(b + 3 - 2C)$, and since both factors must be even in order for b to be integer we must have $b + 3 + 2C = 6$ and $b + 3 - 2C = 2$ which gives $b = C = 1$ and then $a = c - b = C^2 - b = 0$ which was excluded. Thus equality never happens. ■