Math 445 Homework 5

Due Friday, October 10

17. Show that if $a^2 + 2b^2 = c^2$ and $p|(a,c)$ for some prime p, then $p|b$.

    (Note: $p = 2$ is treated differently...)

    If $p|(a,c)$, then $a = px$, $c = py$ for some integers x, y, so $a^2 + 2b^2 = c^2$ implies $2b^2 = c^2 - a^2 = (p^2)(y^2 - x^2)$, so $p^2|2b^2$. If $p = 2$, this in turn implies that, since $4|2b^2$, $2|b^2$ so, since 2 is prime, $2|b$ or $2|b$, so $2|b$. If $p \neq 2$, then $p^2|2b^2$ implies $p|2b^2$, and since $(p,2) = 1$, $p|b^2$, so $p|b$ of $p|b$, so $p|b$.

    So in all cases, p prime and $p|(a,c)$ implies $p|b$.

18. Show that if $a^2 + 2b^2 = c^2$ and $(a,c) = 1$, then a and c are odd, and b is even.

    If a is even, $a = 2x$, then $c^2 = a^2+2b^2 = 4x^2+2b^2 = 2(2x^2+b^2)$ is even, so c is even, so $2|(a,c)$ a contradiction. If c is even, $c = 2y$, then $a^2 = c^2-2b^2 = 4y^2-2b^2 = 2(2y^2-b^2$ is even, so a is even, which is again a contradiction.

    So both a and c are odd, $a = 2k+1$, $c = 2m+1$. If b is odd, $b = 2n+1$, then we have
    $$0 = a^2 + 2b^2 - c^2 = (2k+1)^2 + 2(2m+1)^2 - (2n+1)^2$$
    $$= 4(k^2 + k + 2m^2 + 2m - n^2 - n) + 2$$
    so $0 \equiv 2 \pmod 4$, which is absurd. So b must be even.

19. Continuing the analysis: with $(a,c) = 1$, writing
    $$2b^2 = c^2 - a^2 = (c-a)(c+a) = (2u)(2v) \ ,$$
    show that $(u,v) = 1$, one of u, v is odd and the other even, and $u = 2x^2, v = y^2$ or $u = y^2, v = 2x^2$ for some integers x, y.

    Since both a and c are odd, $c - a = 2u$ and $c + a = 2v$ are both even. Since (adding these two equations) $2c = 2u + 2v$, we have $c = u + v$, and since (subtracting the two equations) $2a = 2v - 2u$, we have $a = v - u$. If $d|u, v$, then $d|u+v, v-u$, so $d|a, c$ so $d|(a,c) = 1$; so the largest integer dividing both u and v is 1, so $(u,v) = 1$.

    Since b is even, $b = 2z$ for some integer z, and then
    $$8z^2 = 2b^2 = c^2 - a^2 = (c-a)(c+a) = (2u)(2v) = 4uv,$$
    so $2z^2 = uv$, so $2|uv$, so $2|u$ or $2|v$; for the sake of concreteness, as assume $2|u$ (the other case is similar). Note that we then cannot have $2|v$, since then $2|(u,v) = 1$. So if u is even, then v is odd (the opposite situation is similar). So $u = 2w$, and $(u,v) = 1$ implies $(w,v) = 1$; anything which divides w and v also divides u and v. Then $2z^2 = uv = 2wv$ implies $z^2 = wv$. Since $(w,v) = 1$, our result from class implies that $w = x^2$, $v = y^2$ for some integers x, y, and so $u = 2x^2$, $v = y^2$, as desired.

    (The opposite case, u odd and v even, yields the other alternative $u = y^2$, $v = 2x^2$.)

20. Finishing the analysis: show that $(2x^2 - y^2)^2 + 2(2xy)^2 = (2x^2 + y^2)^2$, and every solution to $a^2 + 2b^2 = c^2$ with $a, b, c \in \mathbb{N}$ has this form:

$$a = |2x^2 - y^2|,\ b = 2xy,\ c = 2x^2 + y^2, \text{ with } x, y \geq 0 \text{ and } y \text{ odd}.$$

For this problem, the assumption $(a, c) = 1$ was intended to continue....

We have that if $a^2 + 2b^2 = c^2$ with $(a, c) = 1$, then
$a = v - u = y^2 - 2x^2$, $b^2 = 2uv = 4x^2y^2 = (2xy)^2$, so
$b = 2xy$, and $c = v + u = y^2 + 2x^2$

(in the case u even and v odd, <u>or</u>
$a = v - u = 2x^2 - y^2$, $b^2 = 2uv = 4x^2y^2 = (2xy)^2$, so
$b = 2xy$, and $c = v + u = 2x^2 + y^2$

(in the case u odd and v even.

We can unify these two cases by writing $a = |2x^2 - y^2|$, $b = 2xy$, and $c = 2x^2 + y^2$ for integers x, y. So if $a^2 + 2b^2 = c^2$ with $(a, c) = 1$, then $a = |2x^2 - y^2|$, $b = 2xy$, and $c = 2x^2 + y^2$ for integers x, y.

Note that for any integers x, y, these numbers a, b, c <u>do</u> satisfy $a^2 + 2b^2 = c^2$:

$$|2x^2 - y^2|^2 + 2(2xy)^2 = 4x^4 - 4x^2y^2 + y^4 + 8x^2y^2 = 4x^4 + 4x^2y^2 + y^4$$
$$= (2x^2)^2 + 2(2x^2)(y^2) + (y^2)^2 = (2x^2 + y^2)^2 .$$

The last thing to note is that y must be odd; if $y = 2z$, then $2|2(x^2 - 2z^2) = 2x^2 - y^2 = \pm a$ and $2|2(x^2 + 2z^2) = 2x^2 + y^2 = c$, so $2|(a, c) = 1$, a contradiction.