QUIZ 1 SOLUTIONS

27 January 2012

1. (a) Show that if $x^5 + y^5 + z^5 = 0$, then

$$2(x+y+z)^5 = 5(x+y)(x+z)(y+z)\left[(x+y+z)^2 + x^2 + y^2 + z^2\right]$$

Use this to show that 5 divides one of the numbers x, y, z.

(b) Show that Fermat's equation

$$x^5 + y^5 = w^5$$

has no solution when 5 *does not* divide any of the numbers x, y, w.

Solution: (a) This is an exercise in symmetric polynomials. We will make use the binomial formula

$$(a+b)^5 = a^5 + 5a^4b + 10a^3b^2 + 10a^2b^3 + 5ab^4 + b^5 \tag{1}$$

and the fact that

$$a^5 \pm b^5 = (a \pm b)(a^4 \mp a^3b + a^2b^2 \mp ab^3 + b^4). \tag{2}$$

This last equation tells us that

$$a \pm b \mid a^5 \pm b^5 \text{ as polynomials in } a, b. \tag{3}$$

Since we know that $x^5 + y^5 + z^5 = 0$, we see that

$$2(x+y+z)^5 \quad = \quad 2\left[(x+y+z)^5 - (x^5 + y^5 + z^5)\right]$$

We can group together fifth powers to see that the RHS is divisible by $x + y$. Namely, (3) implies that $(x + y) = (x + y + z - z) \mid [(x + y + z)^5 - z^5]$ and $(x + y) \mid (x^5 + y^5)$. So $x + y$ divides their sum, and therefore the RHS.

However a similar argument shows that $x + z$ and $y + z$ divide the RHS. Or if you prefer, since the RHS is symmetric in x, y, z and divisible by $x + y$, it has to be divisible by $x + z$ and$y + z$ as well.

Thus,

$$2\left[(x+y+z)^5 - (x^5 + y^5 + z^5)\right] = (x+y)(x+z)(y+z)P(x,y,z)$$

where $P(x, y, z)$ is some polynomial in x, y, z. We can say more about this polynomial P. It has to again be symmetric in x, y, z. And it has have degree 2 since the degree of LHS is 5 and the degree of the product $(x + y)(x + z)(y + z)$ is 3. That means that P is of the form

$$P(x,y,z) = A(x^2 + y^2 + z^2) + B(xy + yz + zx).$$

All we have to do is determine A and B. To that end, we are going to compare the coefficients of x^4y and x^3y^2 on both sides of the equation

$$2(x+y+z)^5 = (x^2y + xy^2 + y^2z + yz^2 + x^2z + xz^2)\left[A(x^2+y^2+z^2) + B(xy+yz+zx)\right]$$

We use (1) to expand LHS as

$$2(x+y+z)^5 = 2[(x+y)+z]^5$$

Both terms we are interested in do not contain z, so they can only come from $2(x+y)^5$. The coefficient of x^4y is, according to (1), equal to $2\cdot 5 = 10$. On the RHS, the only way we can get x^4y is by multiplying x^2y from the first factor by the x^2 term from the second factor.

As for the term x^3y^2, on the LHS the coefficient is $2\cdot 10 = 20$, cf. (1). On the RHS, we get it by multiplying x^2y from the first factor by the xy term in the second factor; and by multiplying xy^2 from the first factor by the x^2 term in the second factor. The coefficient is therefore $A+B$. To summarize, we have

	LHS	RHS
x^4y	10	A
x^3y^2	20	$A+B$

Hence

$$P(x,y,z) = 10(x^2+y^2+z^2) + 10(xy+yz+xz) = 5(x+y+z)^2 + 5(x^2+y^2+z^2).$$

This proves the desired relation.

The RHS of our relation is divisible by 5, so $5 \mid (x+y+z)$. But that implies that $5^5 \mid (x+y+z)^5$ and therefore

$$5^4 \mid (x+y)(x+z)(y+z)\left[(x+y+z)^2 + x^2+y^2+z^2\right].$$

Assume that 5 does not divide any of the x,y,z. Then $5 \nmid (x+y)(x+z)(y+z)$. So

$$5 \mid (x+y+z)^2 + x^2 + y^2 + z^2.$$

We already know that $5 \mid (x+y+z)$, so 5 must also divide $x^2+y^2+z^2$. Since $x+y+z \equiv 0 \pmod 5$ and $x,y,z \not\equiv 0 \pmod 5$, the only possibilities for $(x,y,z) \pmod 5$ are $(1,1,3)$ or $(1,2,2)$ and their permutations. But that means that $(x^2,y^2,z^2) \pmod 5$ is either $(1,1,4)$ or $(1,4,4)$ or some permutation thereof. In either case $(x^2+y^2+z^2) \not\equiv 0 \pmod 5$, and we get our contradiction.

(b) For this part, if $x^5 + y^5 = w^5$, then $x^5 + y^5 + (-w)^5 = 0$. Part (a) implies that 5 must divide one of the three numbers involved, x, y or $-w$. So 5 must divide x, y or w. Hence there are no solutions to Fermat's equation that have all three numbers not divisible by 5.

2. Find all positive integer solutions to the equation

$$x^2 + 2y^2 = w^2.$$

Solution: Let $d = (x,y,z)$. Then $x = da, y = db, w = dc$ where $(a,b,c) = 1$ and they satisfy the equation

$$a^2 + 2b^2 = c^2.$$

Reducing both sides $\pmod 2$ we see that $a^2 \equiv c^2 \pmod 2$, so a and c must have the same parity. But then $2 \mid (a+c)$ and $2 \mid (a-c)$. Hence $4 \mid (c+a)(c-a) = 2b^2$ and so $2 \mid b$. This, in turn, implies that $8 \mid c^2 - a^2 = (c-a)(c+a)$. Hence $4 \mid (c-a)$ or $4 \mid (c+a)$.

Case 1 $4 \mid c-a$ We still have $2 \mid (c+a)$ and dividing by 8 our equation we see that

$$\left(\frac{b}{2}\right)^2 = \frac{c-a}{4}\frac{c+a}{2}.$$

Each factor on the RHS is an integer. I would like to say that each of them is a square, but for that I need to first show that they are relatively prime. Let $m = \gcd\left(\frac{c-a}{4}, \frac{c+a}{2}\right)$. Then

$$m \mid 2\frac{c-a}{4} + \frac{c+a}{2} = c$$

and

$$m \mid -2\frac{c-a}{4} + \frac{c+a}{2} = a.$$

If m is divisible by 2, it means that both a and c are even. We also know that b is even, and this cannot happen since $(a, b, c) = 1$. If m is divisible by some odd prime p, then $p \mid a$ and $p \mid c$. But then $p \mid 2b^2$ and so p must also divide b, contradicting again the fact that $(a, b, c) = 1$. Hence $m = 1$ and now we can deduce that $c - a = 4u^2$ and $c + a = 2v^2$ for some positive integers $(u, v) = 1$. We obtain

$$\begin{cases} a = v^2 - 2u^2 \\ b = 2uv \\ c = v^2 + 2u^2. \end{cases}$$

Since a and c are odd, v must be odd.

Case 2 $4 \mid c+a$ The same argument applies to $\dfrac{c+a}{4}$ and $\dfrac{c-a}{2}$. We get that $c+a = 4u^2$ and $c-a = 2v^2$ for some positive integers $(u, v) = 1$ and v odd. In consequence,

$$\begin{cases} a = 2u^2 - v^2 \\ b = 2uv \\ c = v^2 + 2u^2. \end{cases}$$

Combining the two cases, we can say that

$$\begin{cases} x = da = d|v^2 - 2u^2| \\ y = db = 2duv \\ z = dc = d(v^2 + 2u^2) \end{cases}$$

with u, v, d positive integers.

Note: If we want to be complete and make sure we only get each solution once, we have to make sure that $(2u^2 - v^2, 2uv, 2u^2 + v^2) = 1$ whenever $(u, v) = 1$ and v is odd. (This was not part of what the problem asked).

If $p \mid (2u^2 - v^2, 2uv, 2u^2 + v^2)$, then $p \mid 4u^2$ and $p \mid 2v^2$. Since $(u, v) = 1$ we can only have $p = 2$. But that would mean that $2 \mid 2u^2 - v^2$, so $2 \mid v$ (contradiction). Thus $(2u^2 - v^2, 2uv, 2u^2 + v^2) = 1$.