ELEMENTARY NUMBER THEORY AND CRYPTOGRAPHY II
SOLUTIONS FOR PROBLEM SHEET 2
EPIPHANY TERM 2015

(1) In all cases there are coprime $s, t \in \mathbb{N}$ such that $s > t$, $s \not\equiv t \pmod 2$, $x = 2st$, $y = s^2 - t^2$ and $z = s^2 + t^2$.

a) Here $st = 15$, therefore $s \equiv t \equiv 1 \pmod 2$ and such Pythagorean triple does not exist.

b) Here $st = 20$, therefore $(s, t) = (20, 1), (5, 4)$ and then triples are $(40, 399, 401)$ and $(40, 9, 41)$.

c) Here $st = 30$, therefore, $(s, t) = (30, 1), (15, 2), (10, 3), (6, 5)$ and the triples are $(60, 899, 901)$, $(60, 221, 229)$, $(60, 91, 109)$, $(60, 11, 61)$.

(2) We can assume that x is even and y is odd. Then there exist coprime $s, t \in \mathbb{N}$ such that $s > t$, $s \not\equiv t \pmod 2$ and

$$x = 2st, \quad y = s^2 - t^2.$$

Therefore, $x + y = (s + t)^2 - 2t^2$ and $x - y = 2t^2 - (s - t)^2$. Now use that $s \pm t$ is odd and therefore $(s \pm t)^2 \equiv 1 \pmod 8$. So, if t is even then $x + y \equiv 1 \pmod 8$ and $x - y \equiv -1 \equiv 7 \pmod 8$. If t is odd then $x + y \equiv -1 \equiv 7 \pmod 8$ and $x - y \equiv 1 \pmod 8$.

(3) Suppose $p_1, p_2, \ldots, p_n$ are different odd primes. Then for $1 \leqslant i \leqslant n$, the natural numbers $s_i = 2p_1 \ldots p_i$ and $t_i = p_{i+1} \ldots p_n$ are coprime, $s_i \not\equiv t_i \pmod 2$ and, therefore, the corresponding Pythagorean triple $(2s_it_i, |s_i^2 - t_i^2|, s_i^2 + t_i^2)$ is primitive. Indeed if $s_i > t_i$ we take $s = s_i$ and $t = t_i$, otherwise we take $s = t_i$ and $t = s_i$. Note that the case $s_i = t_i$ does not occur (why?) It remains to note that for all $1 \leqslant i \leqslant n$, $2s_it_i$ takes the same value $2p_1 \ldots p_n$.

(4) Let r be the radius of the circle, and denote by x, y, z the lengths of the sides of the triangle, where z denotes the length of the hypotenuse. That is we have $x^2 + y^2 = z^2$. Now we observe that the area of the triangle is equal to the sum of the areas of the three triangles having as common vertex the centre of the trainlge. That is we have

$$\frac{1}{2}xy = \frac{1}{2}rx + \frac{1}{2}ry + \frac{1}{2}rz = \frac{1}{2}r(x + y + z)$$

Since any Pythagorean triple can be obtained by a primitive one, by the theorem in the lectures we have that there exist s, t positive integers (with the restrictions as in the theorem) such that $x = k2st$, $y = k(s^2 - t^2)$ and $z = k(s^2 + t^2)$, for some positive integer k. In particular we have

$$r = \frac{xy}{x + y + z} = \frac{2k^2st(s^2 - t^2}{k(2st + s^2 - t^2 + s^2 + t^2)} =$$

$$\frac{kt(s^2 - t^2}{s + t} = kt(s - t) \in \mathbb{N}$$

(5) a) Suppose that $\sqrt{6}$ is rational, i.e. $\sqrt{6} = \frac{p}{q}$. Then the equation $6q^2 = p^2$ has positive integer solutions. Let (p, q) be the solution with the smallest positive integer q. Then p^2 is divisible by 6 i.e. is divisible by 2 and by 3. Therefore p itself is divisible by both 2 and 3. So we have $p = 6p_1$.

Now we can rewrite the equation: $q^2 = 6p_1^2$. By repeating the same arguments we get $q = 6q_1$ and $6q_1^2 = p_1^2$. Finally we have found another solution (p_1, q_1) of the initial equation but with even smaller $q_1 < q$. So we get a contradiction.

b) Method is the same. This time we get the equation $2q^3 = p^3$. Assuming that (p, q) is the solution of the equation with minimal positive q we firstly show that $p = 2p_1$ and then show that $q = 2q_1$. By putting it into the equation we get $2q_1^3 = p_1^3$ so (p_1, q_1) is another solution of the equation with even smaller $q_1 < q$ — a contradiction.

(6) We let x, y, z denote the length of the sides, where z is the hypotenuse. Hence $x^2 + y^2 = z^2$. Assume that the are was a square, say u^2 for some $u \in \mathbb{N}$. Then we would have $\frac{1}{2}xy = u^2$, or equivalently $2xy = 4u^2$. By addining and subtracting to the Pythagorean equation we obtain $(x+y)^2 = z^2+4u^2$ and $(x-y)^2 = z^2 - 4u^2$. After multiplying these two equations,and using the difference of squares identity we obtain

$$(x^2 - y^2)^2 = z^4 - (2u)^4.$$

But we know that the equation $X^4 - Y^4 = Z^2$ does not have a solution in positive integers, hence we have derived a contradiction.

(7) Suppose (x_0, y_0, z_0) is a solution with the smallest possible x_0. Then we firstly show that z_0 and y_0 are coprime. Indeed if some prime $p \neq 2$ divides both y_0 and z_0 then it also divides x_0 and we finally get

$$p^4(x_1^4 - 4y_1^4) = z_0^2.$$

Therefore z_0 is divisible by p^2, $z_0 = p^2 z_1$ and finally $x_1^4 - 4y_1^4 = z_1^2$, so we finally found another solution of the initial equation with $x_1 < x_0$, a contradiction with the choice of (x_0, y_0, z_0).

So, x_0, y_0 and z_0 are coprime. Therefore, $(2y_0^2, z_0, x_0^2)$ is a primitive Pythagorean triple and for some coprime $s > t$, $s \not\equiv t \bmod 2$, we have $y_0^2 = st$ and $x_0^2 = s^2 + t^2$. Using that $\gcd(s, t) = 1$ we obtain by Lemma 3 in the lectures that $s = s_1^2$, $t = t_1^2$ with coprime $s_1, t_1 \in \mathbb{N}$. Therefore, $x_0^2 = s_1^4 + t_1^4$, but this equation has no solutions in positive integers.

(8) Suppose that such triangle exists. Then, $x^2 + y^2 = z^2$ and $xy/2 = 2w^2$ with some $w \in \mathbb{N}$. Then $(x+y)^2 = z^2+8w^2$ and $(x-y)^2 = z^2-8w^2$. Therefore, $(x^2 - y^2)^2 = z^4 - 64w^4$ and we obtained that $z^4 - 4(2w)^4 = (x^2 - y^2)^2$. It remains to apply the statement in Problem 7.

(9) Such Pythagorean triple (x, y, z) should satisfy two equations: $x^2 + y^2 = z^2$ and $xy = 2(x+y+z)$. These equations are symmetric in x and y, therefore it makes sense to introduce the new variables $u = x + y$ and $v = xy$ and to rewrite the above two equations in the form $u^2 - 2v = z^2$ and $v = 2(u + z)$. Eliminating v we obtain $u^2 - 4u = z^2 + 4z$, $(u - 2)^2 = (z + 2)^2$. Since u and v are positive we have $u - 2 = z + 2$ and, finally,

$$u = z + 4, \quad v = 4z + 8.$$

This allows us to find the natural numbers u and v if we start with arbitrary $z \in \mathbb{N}$. But for any given values u and v the values of x and y are the roots of the quadratic equation

$$T^2 - uT + v = T^2 - (z+4)T + 4z + 8 = 0.$$

Therefore, the discriminant

$$u^2 - 4v = (z+4)^2 - 4(4z+8) = z^2 - 8z - 16 = (z-4)^2 - 32$$

must be equal to N^2, where $N \in \mathbb{N}$. So,

$$(z-4)^2 - N^2 = (z-4-N)(z-4+N) = 32$$

and we have the following three cases:

a) $z-4-N = 1$ and $z-4+N = 32$;
b) $z-4-N = 2$ and $z-4+N = 16$;
c) $z-4-N = 4$ and $z-4+N = 8$.

In the case a) there no solutions, in the case b) $z = 13$, $N = 7$ and $(x, y, z) = (12, 5, 13)$, and in the case c), $z = 10$, $N = 2$ and $(x, y, z) = (8, 6, 10)$.

(10) Suppose (x_0, y_0, z_0) is a solution. As usually, we can reduce to the case of primitive solution. Then both x_0 and y_0 are odd and coprime. Then we can set $x_0 - y_0 = 2a$, $x_0 + y_0 = 2b$ and $x_0^2 + y_0^2 = 2c$ with coprime natural numbers a, b and c satisfying the relation $abc = (z_0/2)^2$. This implies that $a = a_1^2$, $b = b_1^2$ and $c = c_1^2$ with $a_1, b_1, c_1 \in \mathbb{N}$. Therefore, $x_0^2 + y_0^2 = (a_1^2 + b_1^2)^2 + (b_1^2 - a_1^2)^2 = 2(a_1^4 + b_1^4)$ implies that $a_1^4 + b_1^4 = c_1^2$. However we have seen in the lectures that this equation has no solutions in the positive integers.