Michaelmas 2012, NT III/IV, Problem Sheet 1.

1. For any natural number n, show an "Euler identity", i.e. that the product of two numbers of the form $x_i^2 + ny_i^2$ $(i = 1, 2)$ is again of that form (i.e. the sum of a square and n times a square).

2. Let $M \in \mathbb{N}$ $(= \{1, 2, 3 \ldots\})$ and write $M = p_1^{m_1} p_2^{m_2} \ldots p_r^{m_r}$ where the p_i are distinct prime numbers and the m_i are positive integers.
   (i) How many pairs (A, B) of *coprime* positive integers are there such that $M = AB$? [*Hint: To obtain a guess for the answer, try to investigate special cases first.*]

   Suppose that $M = AB$ with A and B as in (i).
   (ii) Show that if M is a square (of an integer) then so are A and B.
   (iii) Show, further, that if M is an n^{th} power (of an integer) then so are A and B.

3. Find a formula (similar to that for the Pythagorean triples, given for a coprime triple by $(X, Y, Z) = (2rs, r^2 - s^2, r^2 + s^2)$) giving all the solutions to the equation $X^2 + 2Y^2 = Z^2$ with X, Y and Z in $\mathbb{N}$ and $\gcd(X, Y, Z) = 1$.

4. (i) Show that $X^5 - 3Y^5 = 11$ has no integer solutions. [*Hint: Find the* 5^{th} *powers mod 11.*]
   (ii) Show, using infinite descent, that $3X^4 - 2Y^4 = 55Z^2$ has no integer solutions except $X = Y = Z = 0$. [*Hint: Look mod 5.*]

5. [This exercise finishes off the proof of the 4-squares theorem in the notes.]
   Let p be an odd prime. Show that there are integers a, b, k with $k > 0$ such that
   $$kp = a^2 + b^2 + 1\,.$$
   Hint: Work modulo p. Find the cardinality of the sets $\{a^2 \pmod p \mid 0 \leqslant a \leqslant \frac{p-1}{2}\}$ and $\{-1 - b^2 \pmod p \mid 0 \leqslant b \leqslant \frac{p-1}{2}\}$. Conclude that they have an element in common. (Recall the pigeon-hole principle.)

6. [Infinite descent problems.]
   (i) Show by infinite descent that $\sqrt{N}$ is irrational for any squarefree integer $N > 1$.
   (ii*) Show using infinite descent (or otherwise) that there are no two Pythagorean triples with two lengths in common, i.e. there are no positive integers a, b, c and d such that
   $$a^2 + b^2 = c^2 \quad \text{and}$$
   $$b^2 + c^2 = d^2\,.$$

7. Show: A prime $p > 2$ is a sum of two squares if and only if $p \equiv 1 \pmod 4$.
   Hint: apart from using an "Euler identity",
   - First use congruences to show that $p \equiv 3 \pmod 4$ cannot be a sum of two squares (what do squares of integers look like $\pmod 4$?).
   - Then, for $p \equiv 1 \pmod 4$, try to use the strategy of the proof of the 4-squares theorem.
     i) Show that a (non-zero) multiple of p, say mp, has the desired form $mp = a^2 + b^2$ for some a, b, m. (Put $b = 1$ and use the fact, known from ANTII, that $\mathbb{F}_p^*$, the units in the field with p elements, is a cyclic group. Now use that $p \equiv 1 \pmod 4$.)
     ii) Reduce a solution $mp = a^2 + b^2$, if $m > 1$, to one of the form $m'p = a'^2 + b'^2$, $0 < m' < m$.