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

1. We multiply out

$$(x_1^2 + ny_1^2)(x_2^2 + ny_2^2) = x_1^2x_2^2 + n(x_1^2y_2^2 + x_2^2y_1^2) + n^2y_1^2y_2^2 \qquad (1)$$

and note that the sum of the first and last summand on the right is not too far away from being a square itself:

$$(x_1x_2 \pm ny_1y_2)^2 = x_1^2x_2^2 \ + \ n^2y_1^2y_2^2 \pm 2nx_1x_2y_1y_2\,;$$

for the expression in parentheses above we see a similar expression

$$(x_1y_2 \mp y_1x_2)^2 = x_1^2y_2^2 \ + \ y_1^2x_2^2 \mp 2x_1x_2y_1y_2\,.$$

When adding n times the latter to the former, the two contributions corresponding to the grey terms cancel and we get the RHS of (1). Therefore, our original product has at least two ways in which it can be written in the form (square)+ $n\times$(square):

$$= (x_1x_2 \pm ny_1y_2)^2 \ + \ n(x_1y_2 \mp ny_1x_2)^2\,.$$

2. Write $M = p_1^{m_1}\dots p_r^{m_r}$, where the p_i are distinct primes and $m_i \in \mathbb{N}$, and suppose that $M = AB$ with A and B in N.

Then $A = p_1^{a_1}\dots p_r^{a_r}$ and $B = p_1^{b_1}\dots p_r^{b_r}$ where a_i and $b_i \in \mathbb{N}\cup\{0\}$ and $a_i + b_i = m_i$ for each i.

(i) Suppose $\gcd(A, B) = 1$.

Then, for each $s = 1, \dots, r$, one of a_s and b_s must be 0 and the other m_s. That is $a_s = m_s\epsilon_s$ and $b_s = m_s(1 - \epsilon_s)$ where $\epsilon_s = 0$ or 1. So

$$A = p_1^{m_1\epsilon_1}\dots p_r^{m_r\epsilon_r} \quad \text{and} \quad B = p_1^{m_1(1-\epsilon_1)}\dots p_r^{m_r(1-\epsilon_r)}\,.$$

Thus A and B are uniquely determined by the ϵ_s and each choice of the ϵ_s (to be 0 or 1) gives a different (since the $m_s \neq 0$) coprime pair (A, B) with product M.

So the number of such pairs is 2^r, the number of choices for the ϵ_s.

(ii) and (iii): If M is an nth power then $M = L^n$ for some $L \in \mathbb{N}$.

Since $L \mid M$, the factorization of L involves the same primes as M and so
$L = p_1^{l_1}\dots p_r^{l_r}$,
with $l_i \in \mathbb{N}\cup\{0\}$. Thus
$M = L^n = p_1^{nl_1}\dots p_r^{nl_r}$.
So for each s we have $m_s = nl_s$, and
$A = \left(p_1^{l_1\epsilon_1}\dots p_r^{l_r\epsilon_r}\right)^n$ and $B = \left(p_1^{l_1(1-\epsilon_1)}\dots p_r^{l_r(1-\epsilon_r)}\right)^n$
are nth powers also.

3. Suppose $X,\ Y,\ Z \in \mathbb{N}$, $\gcd(X, Y, Z) = 1$ and $X^2 + 2Y^2 = Z^2$.

Now $\gcd(X, Z) = 1$. ⟦For if some prime p were to divide $\gcd(X, Z)$ then p^2 would divide $X^2 - Z^2 = 2Y^2$ and, even if p were 2, p would divide Y^2 and therefore Y. So p would divide $\gcd(X, Y, Z) = 1$, a contradiction. ⟧

Furthermore, both X and Z are odd. ⟦If one of them were even then the other would be even also (since $2Y^2$ is even) and 2 would be a common factor. ⟧

Thus $Z \pm X$ are both even, and we may put $Z + X = 2D$, $Z - X = 2E$, with D and $E \in \mathbb{Z}$ and $D > E > 0$.

Thus $2Y^2 = Z^2 - X^2 = (Z+X)(Z-X) = 4DE$ is divisible by 4, and hence 2 divides Y. Put $Y = 2T$.

Now the integers D and E are coprime (∗)
⟦since $D + E = Z$ and $D - E = X$ are coprime ⟧.

Moreover $DE = 2T^2$. So one of D and E must be even.

If D is even, then $(D/2)E = T^2$, where the factors on the left are coprime (by (∗)) and positive. So $D/2 = R^2$ and $E = S^2$ for some coprime positive integers R and S.

Similarly, if E is even, then $E/2 = R^2$ and $D = S^2$, for some coprime positive integers R and S.

In either case we find

$$Z = S^2 + 2R^2, \quad X = |S^2 - 2R^2|, \quad Y = 2RS\,,$$

where R and $S \in \mathbb{N}$ and, in fact, $\gcd(2R, S) = 1$ since Z has to be odd.

Now this is the general solution. For it is easily verified that that all such X, Y, and Z satisfy the required conditions, except perhaps the condition $\gcd(X, Y, Z) = 1$. But the latter holds as well; in fact, we have already

$$\begin{aligned} \gcd(X, Z) &= \gcd(2R^2 - S^2, 2R^2 + S^2) = \gcd(2R^2 - S^2, 4R^2) \\ &= \gcd(2R^2 - S^2, R^2) = \gcd(S^2, R^2) = 1\,. \end{aligned}$$

⟦For the second and fourth equalities use that $\gcd(m, n) = \gcd(m, am+n)$. For the third one, note that the $2R^2 - S^2$ is odd. The fifth equality follows since $\gcd(R, S) = 1$. ⟧

4. (i) Note first that the fifth powers modulo 11 are 0 and ±1.
⟦To show this either work out the fifth powers, mod 11, of 0, ±1, ±2, . . . , ±5 (a bit laborious) or, more elegantly, recall that if $T \not\equiv 0 \mod 11$ then, by Fermat's little theorem,

$$(T^5)^2 = T^{10} \equiv 1 \mod 11.$$

Since $\mathbb{Z}_{11}$ is a field, 1 can only have *two* square roots (in fact, ±1) there and so $T^5 \equiv \pm 1$, as required. ⟧

Suppose, then, that we have X and Y in $\mathbb{Z}$ such that $X^5 - 3Y^5 = 11$. Then we would have $X^5 \equiv 3Y^5 \mod 11$.

Now $11 \nmid Y$. ⟦For if $11 \mid Y$ then $11 \mid 11 + 3Y^5 = X^5$, so $11 \mid X$. But then $11^5 \mid X^5 - 3Y^5 = 11$, which is impossible. ⟧

Hence $Y^3 \equiv \pm 1 \mod 11$ and $X^5 \equiv 3Y^5 \equiv \pm 3 \mod 11$. But this is impossible, since $X^5 \equiv 0$ or $\pm 1 \mod 11$. So no such X and Y exist.

(ii) Suppose, for a contradiction, that $3X^4 - 2Y^4 = 55Z^2$ has an integer solution $(X, Y, Z) = (a, b, c)$ other than $a = b = c = 0$.

Let $d = \gcd(a, b)$. We can assume that d is as small as possible. (†)
We claim that 5 does not divide either a or b.

For if $5 \mid a$ then $2b^4 \equiv 0 \mod 5$ and so $5 \mid b$ and then $5^4 \mid (3a^4 + 2b^4) = 55c^2$ so $5^3 \mid c^2$. Whence $5^2 \mid c$. But then $(X, Y, Z) = (a/5, b/5, c/5^2)$ is a new solution with $\gcd(X, Y) < d$ and this contradicts the assumed minimality (†) of d. So $5 \nmid a$, and similarly, $5 \nmid b$.

Now, by Fermat's little theorem (or by finding $n^4 \mod 5$ for $n = 1, 2, 3, 4$), we have $a^4 \equiv b^4 \equiv 1 \mod 5$.

But then, mod 5 we get $0 \equiv 55c^4 \equiv 3a^4 - 2b^4 \equiv 3 - 2 \equiv 1$, and we have the desired contradiction.

5. Put $S_0 := \{a^2 \pmod p \mid 0 \leqslant a \leqslant \frac{p-1}{2}\}$ and
$S_1 := \{-1 - b^2 \pmod p \mid 0 \leqslant b \leqslant \frac{p-1}{2}\}$.

Claim 1: $\big|S_0\big| = \frac{p+1}{2}$.
In other words: we claim that all these residue classes are different.

⟦Suppose $a^2 \equiv (a')^2 \pmod p$ for some $0 \leqslant a, a' \leqslant \frac{p-1}{2}$. (We need to show that $a = a'$.) Then $0 \equiv a^2 - (a')^2 = (a - a')(a + a') \pmod p$, and so $p|(a - a')$ or $p|(a + a')$. But both $a \pm a'$ lie between $-(p-1)$ and $(p-1)$, and the only number in that interval which is divisible by p is 0. Hence we have the *equalities* (not just congruences) $a - a' = 0$ or $a + a' = 0$, of which the latter is only possible for $a = a' = 0$, while the former means $a = a'$. ⟧

Claim 2: $\big|S_1\big| = \frac{p+1}{2}$. This follows in complete analogy with Claim 1 (the differences of elements are the same).

Claim 3: S_0 and S_1 have an element in common.

⟦Put $S = \{\text{all residues mod } p\}$. Then $|S \setminus S_0| = p - \frac{p+1}{2} = \frac{p-1}{2}$ and the pigeonhole principle prevents us from "filling" the remaining $\frac{p-1}{2}$ slots with $\frac{p+1}{2}$ elements in S_1 without "doubling up". Hence S_0 and S_1 must have a non-empty intersection. ⟧

6. (i) Descent for $\sqrt{2}$ irrational: suppose $\sqrt{2}$ is rational, i.e. $\sqrt{2} = \frac{q}{r}$ for some (positive) integers q, r (obviously $q > r$). We can assume q to be smallest possible in such a presentation, and in particular $(q, r) = 1$ ⟦otherwise we could cancel factors and get a smaller q⟧.
From this we will construct a strictly smaller solution (i.e. $\sqrt{2} = \frac{q'}{r'}$ with $q' < q$), which then establishes a contradiction to our assumption that $\sqrt{2}$ is rational.
By squaring our original equation we get

$$2 = (\sqrt{2})^2 = \frac{q^2}{r^2}\,, \qquad \text{hence} \qquad 2r^2 = q^2\,.$$

Since $2|q^2$ and 2 is prime, we find $2|q$ and in fact $2^2|q^2$, and so we find

$$2r^2 = 2^2\Big(\frac{q}{2}\Big)^2, \qquad \text{hence} \qquad r^2 = 2\Big(\frac{q}{2}\Big)^2.$$

Clearly $r > \frac{q}{2}$. Finally we can write

$$2 = \frac{r^2}{(q/2)^2} \qquad \text{hence} \qquad \sqrt{2} = \frac{r}{q/2}$$

and we recall from above that $r < q$.
But q was smallest possible in such a representation of $\sqrt{2}$.

(ii) **Hints:** suppose there are coprime positive integers a, b, c and d with $a^2 + b^2 = c^2$ and $b^2 + c^2 = d^2$, then we can use our knowledge on Pythagorean triples to deduce that i) b must be even; ii) $a = u^2 - v^2$, $b = 2uv$, $c = u^2 + v^2$ as well as $b = 2xy$, $c = x^2 - y^1$ and $d = x^2 + y^2$ for some integers u, v, x, y. iii) x must be odd; iv) define gcd's $e = (x, u)$, $f = (x, v)$, $g = (y, u)$ and $h = (y, v)$ and express x^2 in two ways (one using $u^2 + v^2 + y^2$) in terms of e, f, g, h. v) Now try to construct a smaller quadruple which satisfies two Pythagorean triple equations as above.

7. Case $p \equiv 3 \pmod 4$: For the first claim that a prime $p \equiv 3(4)$ cannot be a sum of two squares, simply note that the residues modulo 4 of squares can only be 0 (for even numbers) or 1 (for odd numbers), and two of these cannot add up to 3 (mod 4).

   i) Check that the following Euler-type identity holds:

$$(a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2 \,.$$

Case $p \equiv 1(4)$:

ii) Claim: $mp = a^2 + 1 \quad$ for some $m \geqslant 1$.

We are allowed to use that $\mathbb{Z}/p\mathbb{Z} \cong \mathbb{F}_p$ is a field with p elements, and that $\mathbb{F}_p^\times = \mathbb{F}_p \setminus \{0\}$ is a cyclic group. In particular we know that the order of a generator, say h, of that cyclic group is $p - 1$. Since $4|(p-1)$, we can form $h^{\frac{p-1}{4}}$ which has order 4 (and behaves like $i = \sqrt{-1}$).

Let H be a representative of the residue class of $h^{\frac{p-1}{4}}$ in $\mathbb{F}_p^\times$, then H^2 is the only non-trivial element of order 2 in $(\mathbb{Z}/p\mathbb{Z})^\times$, so must be $-1 \pmod p$, i.e. $H^2 + 1 \equiv 0 \pmod p$. We can of course choose H to be positive—in fact, we can even choose it $< p$, which entails that we can even impose $0 < m < p$ in the above claim.

iii) The reduction step (successively decrease m in the above claim) now follows very closely the argument for the 4-square theorem. Suppose

$$mp = a^2 + b^2 \qquad \text{for some } a, b \in \mathbb{Z} \,.$$

We can assume that m is odd, since if m is even, then $a \equiv b \pmod 2$ and we find

$$\frac{m}{2} p = \Big(\frac{a+b}{2}\Big)^2 + \Big(\frac{a-b}{2}\Big)^2 \,,$$

with integers on the RHS, so we can replace m by $m/2$.

For m odd we get that a and b must have opposite parity (recall that p is odd). Now we use the clever trick of reducing the statement modulo m instead. We can find $a_0 \equiv a \pmod m$ and $b_0 \equiv b \pmod m$ such that $-m/2 < a_0, b_0 < m/2$.

Then we find that

$$0 < a_0^2 + b_0^2 < 2\frac{m^2}{4} \qquad \text{and} \qquad a_0^2 + b_0^2 \equiv a^2 + b^2 \equiv 0 \pmod m$$

which implies that

$$a_0^2 + b_0^2 = km \qquad \text{with} \qquad k < \frac{m}{2} \,.$$

Finally use the Euler-type identity above to deduce that

$$km \cdot mp = (a_0^2 + b_0^2)(a^2 + b^2) = (a_0 b - b_0 a)^2 + (a_0 a + b_0 b)^2$$

and note that $m|(a_0 b - b_0 a)$ as well as $m|(a_0 a + b_0 b)$. This allows us to divide both sides by m^2 while still retaining an equality $kp = r^2 + s^2$ with *integers* r, s, and in fact with a multiple k on the LHS which is smaller than the one we started out with (viz. m). After finitely many steps, we arrive at $k = 1$ and we have found a presentation of p as a sum of two squares.