The following questions, or parts of questions, count for assessment: 1, 2, 3, 4 (odd-numbered parts), 5, 6 (odd-numbered parts), 8, 11, 12. These are marked *. Please hand in your solutions, via the Coursework Box on Level 8 of the Laver Building, by Friday 7th February.

1*. Find all quadratic residues a mod p (in the range $-\frac{1}{2}p < a < \frac{1}{2}p$) for $p = 17$, 19 and 23. **[9]**

2*. Let p be a prime with $p \equiv 3 \pmod 4$. Show that if $p \nmid a$ and the congruence $x^2 \equiv a \pmod p$ is soluble then its solution is $x \equiv \pm a^{(p+1)/4}$. Hence solve $x^2 \equiv 5 \pmod{79}$. [Hint: Use Euler's Criterion.] **[8]**

3*. Use Gauss' Lemma to compute the following Legendre symbols:
(i) $\left(\frac{7}{11}\right)$; (ii) $\left(\frac{5}{13}\right)$; (iii) $\left(\frac{-3}{17}\right)$; (iv) $\left(\frac{5}{19}\right)$. **[12]**

4. Evaluate each of the following Legendre symbols using quadratic reciprocity. (The numbers underneath are all primes.)
(i)* $\left(\frac{3}{53}\right)$; (ii) $\left(\frac{7}{79}\right)$; (iii)* $\left(\frac{15}{101}\right)$; (iv) $\left(\frac{31}{641}\right)$;
(v)* $\left(\frac{111}{991}\right)$; (vi) $\left(\frac{105}{1009}\right)$; (vii)* $\left(\frac{77}{107}\right)$; (viii) $\left(\frac{133}{191}\right)$;
(ix)* $\left(\frac{-111}{257}\right)$; (x) $\left(\frac{221}{347}\right)$; (xi)* $\left(\frac{-257}{541}\right)$; (xii) $\left(\frac{511}{881}\right)$. **[18]**

5*. Find all solutions in integers to the following Diophantine equations (or show that there are none):
(i) $3x + 5y = 7$;
(ii) $4x - 6y = 3$;
(iii) $4x - 6y = 10$;
(iv) $x^2 - 7y = 4$;
(v) $x^2 + 4y^2 = 25$;
(vi) $x^2 + 1 = 7y^2 + 14x^3y^4$;
(vii) $x^2 - y^2 = 15$.

[17]

6. For each of the following numbers n, determine whether n can be written as the sum of two squares and, if it can, write n in that form.
(i)* 34; (ii) 53; (iii)* 67; (iv) 73; (v)* 99; (vi) 229;
(vii)* $3185 = 5 \cdot 7^2 \cdot 13$; (viii) $5075 = 5^2 \cdot 7 \cdot 29$; (ix)* $39690 = 2 \cdot 3^4 \cdot 5 \cdot 7^2$.
[10]

7. Let p be a prime with $p \equiv 1 \pmod 4$. Show that the represention of p as the sum of two squares is unique, up to signs and the order of the summands, i.e. that if $p = a^2 + b^2 = c^2 + d^2$ with a, b, c, d all *positive* then either $a = c$, $b = d$ or $a = d$, $b = c$.
[Hint: Show that $(ad-bc)(ad+bc) = p(d^2-b^2) \equiv 0 \pmod p$ and use the fact that $0 < a, b, c, d < \sqrt{p}$, together with fact that $p^2 = (ac-bd)^2 + (ad+bc)^2$, to deduce that either $ad = bc$ or $ac = bd$.]

8*. If $n = a^2 + b^2$, we will regard any of the 8 expressions $(\pm a)^2 + (\pm b)^2$ and $(\pm b)^2 + (\pm a)^2$ for n as equivalent to $a^2 + b^2$. Find two inequivalent expressions for $377 = 13 \cdot 29$ as the sum of two squares. Do the same for $3869 = 53 \cdot 73$. Find four inequivalent representations of $112201 = 29 \cdot 53 \cdot 73$. **[10]**

9. Show that a positive integer n can be expressed as the difference of two integer squares if and only if $n \not\equiv 2 \pmod 4$.

10. Write 29 and 43 as sums of 4 squares, and hence write $1247 = 29 \cdot 43$ in that form.

11*. Show that if $n \geq 170$ then n can be written as the sum of 5 *positive* squares. [Hint: Write $m = n - 169$ as a sum of 4 integer squares and use the fact that $169 = 13^2 = 5^2 + 12^2 = 3^2 + 4^2 + 12^2 = 1^2 + 2^2 + 8^2 + 10^2$.] **[8]**

12*. Show that in every Pythagorean triple (x, y, z), at least one of x, y is divisible by 3, and at least one of x, y, z is divisible by 5. **[8]**

13. Prove or disprove the following statement: If (x, y, z) is a Pythagorean triple (not necessarily primitive) then, after swapping x and y if necessary, there are integers r, s such that $x = r^2 - s^2$, $y = 2rs$, $z = r^2 + s^2$.

Nigel Byott
December 2002