Question 10

(i) Since $x^2 \equiv a \pmod p$, it follows from Euler's criterion (Theorem 9.2) that $a^{(p-1)/2} \equiv 1 \pmod p$. 1

If $x \equiv \pm\, a^{(p+1)/4} \pmod p$, then

$$x^2 \equiv a^{(p+1)/2} \equiv a^{(p+1)/2} \cdot a^{(p-1)/2} \equiv a^p \equiv a \pmod p,$$ 3

the last step following from Fermat's theorem.

(ii) (a) Since 19 and 43 are prime numbers congruent to 3 (mod 4), we can use part (i). The solutions to $x^2 \equiv -2 \pmod{19}$ are $x \equiv \pm\ \pmod{19}$ — that is, $x \equiv 6$ or $13 \pmod{19}$. 2

The solutions to $x^2 \equiv -2 \pmod{43}$ are $x \equiv \pm\, 2^{11} \pmod{43}$ — that is, $x \equiv 16$ or $27 \pmod{43}$. 3

(b) We use the Chinese Remainder Theorem for simulataneous congruences. 1

[*Total: 10 marks*]

Question 11

(i) Since $(r|p) = (p - r|p)$, we have 1

$$S = \sum_{(r|p)=1} r = \sum_{(r|p)=1} (p - r).$$ 1

Thus $2S = \sum_{(r|p)=1} p = p(p-1)/2.$ 2

So $S = p(p-1)/4$.

(ii) $\sum r^3(r|p) = \sum (p-r)^3(r|p)$ 1

$$= p^3 \sum (r|p) - 3p^2 \sum r(r|p) + 3p \sum r^2(r|p) - \sum r^3(r|p).$$ 1

But $\sum (r|p) = 0,$ 1

and $\sum r(r|p) = \sum (p-r)(r|p) = p \sum (r|p) - \sum r(r|p),$ 2

so $\sum r(r|p) = 0.$

So $2 \sum r^3(r|p) = 3p \sum r^2(r|p)$, and the result follows. 1

[*Total: 10 marks*]

Question 12

Your account should include most of the following:

(i) the definition of a Dirchlet character mod k;

(ii) the distinction between the principal character and non-principal characters;

(iii) the number of Dirichlet characters mod k;

(iv) the multiplicative and periodic properties of Dirichlet characters;

(v) the orthogonality relation (Theorem 6.16);

(vi) the non-vanishing of $L(1, \chi)$ for real nonprincipal χ;

(vii) asymptotic formulas involving Dirichlet characters;

(viii) mention of the use of Dirichlet characters in the proof of Dirichlet's theorem on primes in arithmetic progressions.

[*Total: 10 marks*]