1. (i)

$$(34, 21) = (21, 13) = (13, 8) = (8, 5) = (5, 3) = (3, 2) = (2, 1) = 1.$$
$$(89, 55) = (55, 34) = (34, 21) = \cdots = 1.$$
$$13 \times 34 - 21 \times 21 = 1.$$

Application of Euclid's algorithm. [7 marks]

(ii) $(F_n, F_{n-1}) = (F_{n-1}, F_{n-2})$ because $F_{n-2} = F_n - F_{n-1}$ and $(a, b) = (a + kb, b)$ for any a and b. *Application of result from lectures.* [3 marks]

So $(F_n, F_{n-1}) = \cdots = (F_1, F_0) = (1, 1) = 1$. (Induction isn't really necessary.) *Basic logic.* [3 marks]

(iii) We know that $r_n \geq 1$ since it is not zero, and so $r_{n-1} \geq 1$ as well. So $r_n \geq F_0$ and $r_{n-1} \geq F_1$. At each stage, we have $r_{i-1} = q_i r_i + r_{i+1} \geq r_i + r_{i+1}$, because $q_i \geq 1$. So by induction $r_{n-i} \geq F_i$, and therefore $a = r_0 \geq F_n$. *Unseen.* [6 marks]

The final statement is simply the contrapositive of the one just proved. *Basic logic.* [1 marks]

2. (i) Fermat's theorem: if p is prime, then $a^p \equiv a \pmod{p}$ for any integer a. *Bookwork.* [2 marks]

Taking $p = 5$, we get $a^5 \equiv a \pmod 5$. If $5 \nmid a$, then cancel a from both sides to get $a^4 \equiv 1 \pmod 5$. If $5 \mid a$, then both sides are 0. Either way, $a^4 \equiv 0$ or $1 \pmod 5$. *Similar to examples in lectures.* [2 marks]

First calculate

$$2^{2006} = 2^{4\times 501+2} \equiv 1^{501} \times 2^2 = 4 \pmod 5.$$

But each of x^4 and y^4 is either 0 or 1 modulo 5, so their sum cannot equal 4 (either by trying all cases, or just by saying it's obvious). Deduce there are no solutions to the equation. *Similar to example in lectures.* [4 marks]

(ii)

$$(x+4)^4 = x^4 + 4 \times 4x^3 + 6 \times 16x^2 + 4 \times 4^3 x + 4^4 \equiv x^4 \pmod{16}.$$

Similar to example in lectures. [2 marks]

By previous identity, to find all values of n^4 modulo 16 we only need to look at 0^4, 1^4, 2^4 and 3^4. These are 0, 1, 0, 1 respectively. So the possible values are 0 and 1. *Similar to example in lectures.* [4 marks]

(iii) We have $n^4 \equiv 0, 1 \pmod 5$ and $n^4 \equiv 0, 1 \pmod{16}$. Now (5, 16)=1 so each pair of possibilities gives a unique solution modulo 80 (Chinese Remainder Theorem).

If $n^4 \equiv 0 \pmod 5$ and $n^4 \equiv 0 \pmod{16}$ then $n^4 \equiv 0 \pmod{80}$.

If $n^4 \equiv 1 \pmod 5$ and $n^4 \equiv 1 \pmod{16}$ then $n^4 \equiv 1 \pmod{80}$.

If $n^4 \equiv 0 \pmod{16}$ then it is one of $0, 16, 32, 48, 64 \pmod{80}$ and the only one of these which is $1 \pmod 5$ is 16.

If $n^4 \equiv 1 \pmod{16}$ then it is one of $1, 17, 33, 49, 65 \pmod{80}$ and the only one of these which is $0 \pmod 5$ is 65.

So the answers are 0, 1, 16 and 65, all modulo 80. *Similar to example in lectures.* [6 marks]

3. (i) Start with $k = n-1$ and compute $b^k \pmod{n}$. If it not 1 then fail. While k is even, halve k and compute $b^k \pmod{n}$. Fail if we ever find $b^{2k} \equiv 1 \pmod{n}$ but $b^k \not\equiv \pm 1 \pmod{n}$. Otherwise pass. *Bookwork.* [3 marks]

If n is prime, then $b^{n-1} \equiv 1 \pmod{n}$ by Fermat and the only square roots of 1 are ± 1, so n passes the test. *Bookwork.* [2 marks]

(ii) (a) $2^{10} = 1024 \equiv 1 \pmod{341}$ (probably using a calculator) and so 2^{340} and 2^{170} are both $1 \pmod{341}$. But $2^{85} \equiv 2^5 = 32$ so we fail the test. Conclude that 341 is a pseudoprime to the base 2 but not a strong pseudoprime, and so not prime.

(b) $3^5 = 243 \equiv 1 \pmod{121}$ and so 3^{120}, 3^{60}, 3^{30} and 3^{15} are all $1 \pmod{121}$. Test passed, so 121 is a strong pseudoprime to base 3, but not prime since it is 11^2.

(c) $2^{24} = 16777216 \equiv 1 \pmod{221}$ and so $2^{220} = 2^{9\times 24+4} \equiv 2^4 = 16 \pmod{221}$. Test failed, so not a pseudoprime to base 2 and certainly not a strong pseudoprime. *Similar to examples in lectures.* [9 marks]

(iii) Let $x = b^r$. We have $x^2 \equiv 1 \pmod{n}$ but $x \not\equiv \pm 1 \pmod{n}$. Now $(x-1, n)$ is certainly a factor of n. If it is equal to n, then $n \mid (x-1)$ so $x \equiv 1 \pmod{n}$. If it is equal to 1, then $n \mid (x^2-1)$ implies $n \mid (x+1)$ so $x \equiv -1 \pmod{n}$. Conclude that $(x-1, n)$ must be a proper factor of n. *Result from lectures, after putting $x = b^r$.* [4 marks]

Taking $n = 341$ and $b = 2$, we have $32^2 \equiv 1 \pmod{341}$ and so $(31, 341) = 31$ and $(33, 341) = 11$ are proper factors of 341. [2 marks]

4. (i) In $n! = n \times (n-1) \times \cdots 2 \times 1$ there are $\left[\frac{n}{p}\right]$ factors which are multiples of p, $\left[\frac{n}{p^2}\right]$ which are multiples of p^2, and so on. As p is prime, no powers of p can come from anywhere else. So the formula holds. *Bookwork.* [2 marks]

This gives that the power of 5 dividing 2006! is $401 + 80 + 16 + 3 = 500$. The power of 2 is greater, so the number of zeroes is 500. *Similar to examples.*

[2 marks]

The formula gives $28! = 2^{25} \times 5^5 \times \cdots$, $20! = 2^{18} \times 5^4 \times \cdots$ and $8! = 2^7 \times 5^1 \times \cdots$. Putting this together gives $\binom{28}{8} = 2^0 \times 5^0 \times \cdots$ so there are no zeroes. (Could have got this by looking just at 5's or just at 2's.) *Similar to examples.* [4 marks]

(ii) $\phi(n)$ is the number of integers in $\{1, \ldots, n\}$ which are coprime to n. In $\{1, \ldots, p^r\}$ there are p^{r-1} multiples of p and these are the only numbers not coprime to p^r, hence the formula. In general,

$$\begin{aligned}\phi(n) &= p_1^{n_1-1}(p_1 - 1) \times \cdots \times p_k^{n_k-1}(p_k - 1) \\ &= n(1 - \frac{1}{p_1}) \cdots (1 - \frac{1}{p_k}).\end{aligned}$$

Either is OK, or any variant. *Bookwork.* [5 marks]

(iii) We have

$$\phi(100!) = \prod_{5 \neq p \leq 100} p^{v_p - 1}(p-1) \times 5^{v_5 - 1} \times 4$$

where v_p is the exponent of the greatest power of p dividing 100!. The 5's in this come from the 5^{v_5-1}, and from the $(p-1)$s for $p = 11, 31, 41, 61, 71$. By the previous formula, $v_5 = 24$ so the answer is $24 - 1 + 5 = 28$. *Unseen.* [7 marks]

5. (i) Each line shows that $r_{j+1} \equiv 10r_j \pmod{m}$, so (by induction?) $r_j \equiv 10^{j-1} \pmod{m}$. There are only finitely many residues mod m, so we must have $r_i = r_{i+k}$ for some $i \geq 1$ and $k \geq 1$. Let i be the least such, and suppose that $i > 1$. Then $10^i \equiv 10^{i+k} \pmod{m}$ and since $(10, m) = 1$ we may divide by 10 to get $10^{i-1} \equiv 10^{i-1+k} \pmod{m}$, contradicting minimality. So $i = 1$. Now let k be the least such that $r_{1+k} = r_1 = 1$; then k is the least such that $10^k \equiv 1 \pmod{m}$, which by definition is the order of 10 modulo m. *Bookwork.* [7 marks]

(ii) Compute that $\mathrm{ord}_7(10) = 6$ and $\mathrm{ord}_{13}(10) = 6$. Using the hint, $10^8 \equiv -1 \pmod{17}$ so $10^{16} \equiv 1 \pmod{17}$. So $\mathrm{ord}_{17}(10)$ divides 16 but not 8, so is 16. *Similar to examples.* [7 marks]

(iii) If p is prime, then $\mathrm{ord}_p(10) = p - 1$ if and only if 10 is a primitive root modulo p, by definition. *Almost bookwork.* [6 marks]

6. (i) $d(n)$ is the number of divisors of n. $\sigma(n)$ is the sum of the divisors of n. The divisors of p^a are p^k for $1 \le k \le a$, so their sum is $1 + \cdots + p^a$. This is equal to $(p^{a+1} - 1)/(p-1)$ as can be checked by multiplying out.

σ is multiplicative means that if $(m, n) = 1$ then $\sigma(mn) = \sigma(m)\sigma(n)$. It is true because any divisor d_i of mn splits uniquely into the product of a divisor x_i of m and a divisor y_i of n, and then

$$\left(\sum_{d|m} d\right) \times \left(\sum_{d'|n} d'\right) = \sum_{dd'|mn} dd'.$$

Using these two facts, we get

$$\sigma(p_1^{n_1} \times \cdots \times p_k^{n_k}) = \frac{p_1^{n_1+1} - 1}{p_1 - 1} \cdots \frac{p_k^{n_k+1} - 1}{p_k - 1}.$$

Bookwork. [9 marks]

(ii) Table of $\sigma(p^a)$:

	2	3	5	7
1	3	4	6	8
2	7	13	31	57
3	15	40		
4	31			

and then $\sigma(p) = p + 1$ for $11 \le p \le 59$. We must make up 60 by taking products of numbers from separate columns. So

$$\begin{aligned} \sigma(59) &= 60 \\ \sigma(38) = \sigma(19 \times 2) &= 20 \times 3 = 60 \\ \sigma(24) = \sigma(3 \times 2^3) &= 4 \times 15 = 60. \end{aligned}$$

Similar to examples. [5 marks]

(iii) A perfect number is a number n satisfying $\sigma(n) = 2n$ or equivalently $s(n) = n$. Suppose that $n = 2^s(2^{s+1} - 1)$ with $2^{s+1} - 1$ prime. Then

$$\begin{aligned} \sigma(n) &= \sigma(2^s)\sigma(2^{s+1} - 1) \\ &= (1 + 2 + \cdots + 2^s)2^{s+1} \\ &= (2^{s+1} - 1)2^{s+1} \\ &= 2 \times 2^s(2^{s+1} - 1) \\ &= 2n \end{aligned}$$

so n is a perfect number. *Bookwork.* [4 marks]

Putting $s = 1, 2, 4$ we get 6, 28, 496. [2 marks]

7. (i) The convergents of x_0 are the rational numbers

$$a_0, \quad a_0 + \frac{1}{a_1}, \quad a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2}}, \quad a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3}}}, \quad \ldots.$$

Alternatively, they may be defined as p_k/q_k where p_k and q_k satisfy the relations

$$p_0 = a_0, q_0 = 1, p_1 = a_0 a_1 + 1, q_1 = a_1,$$
$$p_{k+1} = a_{k+1} p_k + p_{k-1}, q_{k+1} = a_{k+1} q_k + q_{k-1}.$$

Bookwork. [3 marks]

The continued fraction for π is $[3, 7, 15, 1, \ldots]$. The first four convergents of π are 3, 22/7, 333/106, 355/113. [I have checked that the standard University calculator has enough precision to do this calculation.] *With calculator, from definition.* [3 marks]

(ii) If $Q_k = 1$ then $x_k = P_k + \sqrt{n}$ so $a_k = [x_k] = P_k + [\sqrt{n}] = P_k + a_0$. Then $P_{k+1} = a_k - P_k = a_0 = P_1$ and $Q_{k+1} = n - P_{k+1}^2 = n - P_1^2 = (n - P_1)^2/Q_0 = Q_1$. So both P_k and Q_k recur, and hence so do x_k and a_k. *Bookwork.* [6 marks]

(iii) Work out the continued fraction for $\sqrt{18}$.

k	P_k	Q_k	x_k	a_k	p_k	q_k
0	0	1	$\sqrt{18}$	4	4	1
1	4	2	$\frac{4+\sqrt{18}}{2}$	4	17	4
2	4	1	$4+\sqrt{18}$	8	140	33
3	4	2	$\frac{4+\sqrt{18}}{2}$	4	577	136
4	4	1	$4+\sqrt{18}$	8	4756	1121
5	4	2	$\frac{4+\sqrt{18}}{2}$	4	19601	4620

Solutions come from odd k for which $Q_{k+1} = 1$. So $(x, y) = (17, 4)$, $(577, 136)$, $(19601, 4620)$. *Similar to examples.* [8 marks]

8. (i) n is a quadratic residue modulo p if there exists an integer x such that $x^2 \equiv n \pmod p$. *Bookwork.* [2 marks]

Since $6^2 \equiv -1 \pmod{37}$, -1 is a quadratic residue modulo 37. *Understanding of definition.* [2 marks]

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4 \\ -1 & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

Bookwork. [2 marks]

In the previous part, $37 \equiv 1 \pmod 4$ and -1 is a quadratic residue modulo 37, in accordance with what we have just proved. *Application of result.* [1 marks]

(ii) Gauss' law of quadratic reciprocity: if p and q are distinct odd primes, then

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4 \text{ or } q \equiv 1 \pmod 4; \\ -1 & \text{if } p \equiv 3 \pmod 4 \text{ and } q \equiv 3 \pmod 4. \end{cases}$$

(Any other way of stating it is equally acceptable.) *Bookwork.* [3 marks]

So

$$\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod 5; \\ -1 & \text{if } p \equiv \pm 2 \pmod 5. \end{cases}$$

Simple application of result. [2 marks]

(iii) Suppose x and y are coprime, and that p is an odd prime, not equal to 5, such that $p \mid (x^2 - 5y^2)$. If $p \mid x$ then $p \mid x^2$ so $p \mid 5y^2$ and then, since $p \nmid 5$, $p \mid y^2$ and hence $p \mid y$. This contradicts $(x, y) = 1$ so cannot be true, i.e. $p \nmid x$. Similarly $p \nmid y$.

Since $p \nmid y$, we have $(p, y) = 1$ and so y has an inverse modulo p, i.e. there exists an integer s such that $sy \equiv 1 \pmod p$. So taking $p \mid (x^2 - 5y^2)$, we get $x^2 \equiv 5y^2 \pmod p \implies s^2x^2 \equiv 5 \pmod p$ so 5 is a quadratic residue modulo p. Deduce that $p \equiv \pm 1 \pmod 5$. *Unseen.* [8 marks]