Notes on 2011 Exam

Most of this exam is probably perfectly do-able – but the proportion of bookwork is probably somewhat higher than you will encounter this year, and it occurs in longer segments. The examined syllabus this year is, however, larger than last year.

1. Parts (i) to (iii) are standard bookwork – but no proof was given in this year's course of the "theorem on division with remainder" This theorem says that if n is any integer and q is any nonzero integer, then there are integers a and r such that $n = aq + r$ and $0 \leq r < |q|$.

2. For an integer a and prime p, the notation $\mathrm{ord}_p(a)$ simply means the largest integer $k \geq 0$ such that p^k divides a. No proof is given in the solutions of the uniqueness of prime factorisation (part (iii)) so I am not sure exactly what was intended.

6. (i) This uses the fact that $\phi(r)$ is even for any integer r which is greater than 2. From the solution, one is allowed to assume this. It is treu because either r is divisible by a prime $p > 2$ – in which case $p - 1 = \phi(p)$ is even and divides $\phi(r)$ – or $r = 2^k$ for $k \geq 2$ and then $\phi(r) = 2^{k-1}$ is even.

Notes on 2003 Exam

1. This question simply tests understanding of modulo arithmetic. Remember that $x \equiv 0 \mod p$ simply means that x is divisible by p. It is understood that x is an integer.

2. This question tests Fermat's Little Theorem – all the way through.

3. This is about the Euler ϕ function. Remember the multiplicative properties of this function. It n_1 and n_2 are coprime then $\phi(n_1 n_2) = \phi(n_1)\phi(n_2)$.

4. This is about the Miller Rabin Test. A strong pseudo-prime is simply a composite number (a non-prime) which passes the Miller Rabin Test. The notation (a, n) means the gcd of a and n.

5. not on the syllabus this year.

6. $d(n)$ is simply the number of positive divisors of n, $\sigma(n)$ was the notation used in the 2033 course for the sum of the divisors of n – which was called $\int n$ this year. This question should be do-able.

7. Not on the syllabus this year.

8. Euler's Criterion for quadratic residues is simply the equation

$$\left(\frac{a}{p}\right) = a^{(p-1)/2}$$

if p is an odd prime and a is coprime to p.

8(iii) – which is bookwork — strikes me as quite long, but the exercises which follow are quite short.

Notes on 2004 exam

1. (α, β) means the gcd of integers α and β.

2. In part (ii), you are expected to use the facts that $\phi(n_1n_2) = \phi(n_1)\phi(n_2)$ if n_1 and n_2 are coprime, and that if a is any fixed strictly positive integer then $\phi(p^a)$ is strictly increasing in primes p, and for a fixed prime p, $\phi(p^a)$ is strictly increasing in the integer variable a.

3. The definition of Carmichael number used here is the same as used in this year's course. Part (i) should say that the q_i are distinct *odd* primes.This part of the question is therefore simply asking for a proof that Korsellt's Criterion for a Carmichael number is sufficient.

4. Not on the syllabus this year

5. The notation $\sigma(n)$ is used here for the sum of divisors of n. In this year's course the notation $\int(n)$ was used.This question is about perfect numbers, and should be do-able.

6. Miller's test is what was called the Miller-Rabin test in this year's course. This question should be do-able.

7. This was not on the syllabus this year.

8. See notes on 2003 exam for what is meant by Euler's criterion for quadratic reciprocity.