

1996 Paper 13 Question 13

Complexity Theory

One version of the algorithm that uses discrete Fourier Transforms when multiplying integers uses modular arithmetic for much of its internal working. The modulus involved will be chosen to be one greater than a power of two. Explain why this is the case, what power of two is involved, how this relates to the number of digits in the numbers being multiplied and how the basic operations of modular arithmetic are performed. Does it matter that the modulus used is usually not a prime number?

[20 marks]