

Applied Algebra

Instructions Please write your name in the upper right-hand corner of the page. Use complete sentences, along with any necessary supporting calculations, to answer the following questions.

1. Find the order of 22 modulo 23, that is, find the smallest positive integer k such that $22^k \equiv 1 \pmod{23}$.

Applied Algebra

2. You receive a message that was encoded by the RSA system using public key $(55, 3)$, where 55 is the modulus n and 3 is the exponent a . The coded message, in two blocks, is 20 11. Decode the message and convert the result into alphabetic form via the correspondence $A \leftrightarrow 1$, $B \leftrightarrow 2$, etc.

[Hints: Notice that $\phi(55) = 40$. Also, the easy way to do computations mod 55 is to compute both mod 5 and mod 11 and then use the Chinese remainder theorem.]