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 $22^k \equiv 1 \mod 23$.

   Solution. Observe that $22^2 \equiv (-1)^2 \equiv 1 \mod 23$, so the order of 22 is 2.

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.]

   Solution. You know that $\phi(55) = \phi(5)\phi(11) = 4 \times 10 = 40$, and the first step is to find a multiplicative inverse of 3 mod 40. Either by the Euclidean algorithm or by the matrix method or by inspection, you can see that $3 \times (-13) \equiv 1 \mod 40$. Since you would like to have a *positive* exponent for decoding, it is preferable to use the value 27 (because $-13 \equiv 27 \mod 40$) as the decoding exponent.

   The first block of the message decodes as $20^{27} \mod 55$. This calculation looks nasty to do by brute force. But observe that $20^{27} \equiv 0 \mod 5$, and $20^{27} \equiv 9^{27} \equiv 3^{54} \equiv 3^4 \mod 11$ by Fermat's theorem, and $3^4 \equiv 81 \equiv 4 \mod 11$. Consequently, the congruence $20^{27} \equiv t \mod 55$ is equivalent to the pair of simultaneous congruences $t \equiv 0 \mod 5$ and $t \equiv 4 \mod 11$. You do not need the full power of the Chinese remainder theorem here, for you can see by inspection that $t = 15$ works.

   The second block of the message decodes as $11^{27} \mod 55$. You can now argue as in the preceding paragraph. Alternatively, observe that $11^2 = 121 \equiv 11 \mod 55$, so $11^k \equiv 11 \mod 55$ for every positive integer k. Thus the second block decodes as 11.

   Since O is the 15th letter of the alphabet, and K is the 11th letter, the decoded message 15 11 translates into the alphabetic message OK.