

Math 126
Problem set 07
REVISED TUE MAR 31

Problems to be turned in: 16.3, 17.1, 17.5(a,b), 18.1, and:

1. Implement the successive squaring algorithm in either Excel, Google spreadsheets, or a standard computer language of your choice (either compiled or interpreted). Some notes:
 - You can use either the version described in Algorithm 16.1, the version described in Exercise 16.2, or the spreadsheet version shown in class (which is basically the version in Exercise 16.2).
 - Your program should accept all values of k whose binary digits go up to the $2^{22} = 4194304$ place (i.e., $1 \leq k \leq 2^{23} - 1$).

When you submit your homework, include (either on paper or electronically) both the source code for your program and at least one example. If you do your program in Excel or Google spreadsheets, the following links describe how to print your cell formulas, which will be your “source code”:

<http://www.wikihow.com/Print-Cell-Formulas-Used-on-an-Excel-Spreadsheet>
<https://support.google.com/docs/answer/139561?hl=en>
<https://productforums.google.com/forum/#!topic/docs/gGoEJrsnpCU>

2. Encode a message using $k = 23427$ and $m = 744193$. Make sure your message is at least 8 letters long, in groups of 2 letters. Submit your original message and the encoded version. (For those with too much time on their hands and access to a computer: Try to figure out the exponent that will decode messages encoded with the above values of k and m .)

Note that 17.3(a,c) is no longer assigned. Note also that the numbers are much smaller than in the previous version, as integer multiplication in Excel is only reliable up to 7-digit numbers (or so).