Math 116
Homework 7 Solutions

I graded 4 of the problems: 2, 4, 8, 10.

Each problem is worth 3 points. A grade of 0 indicates no solution or a substantially wrong solution. A grade of 3 indicates a correct or nearly correct solution. Otherwise the grade given is 1 or 2 depending upon how much work was put in and how close the solution is to being correct. How neat and clear your solution is also affects the grade I give.

If you believe a problem was misgraded, or I made some addition or other error, please write a short note explaining the situation, attach it to your homework, and return it to me (either in person, in my mailbox, or under my office door). I'll take a look and return the homework in the next section.

The following are solutions to the homework problems (excepting problems whose solutions are in the back of the text) and additional comments for the problems I graded.

General Comments
The maximum number of points was 12. The high score was 12, the median was 11 and the mean was 10.2. Everyone did well on this assignment and there were many perfect scores.

2. Factor $437 = pq = 19 \cdot 23$. Then $(p-1)(q-1) = 18 \cdot 22 = 2^2 \cdot 3^2 \cdot 11 = 396$. The possible encryption exponents (up to congruence mod 396) are all numbers between 1 and 396 that are relatively prime to 396; these are all numbers which have an inverse mod 396. Notice that 1 is not a very good choice for an encryption exponent, since it would be a little too easy to decrypt, but it's still possible! So there are $\phi(396) = \phi(2^2) \cdot \phi(3^2) \cdot \phi(11) = 2 \cdot 6 \cdot 10 = 120$ possible encryption exponents. In general for $n = pq$ there are $\phi((p-1)(q-1))$ possible encryption exponents.

   Comments: Many people disallowed the encryption exponent $e = 1$, which is fine. The wording in the book implied you should list the 120 (or 119) possible encryption exponents, and a few people did, but I certainly did not expect you to do so. Just indicating how you would determine which numbers are possible encryption exponents and which are not was fine.

4. Factor $899 = pq = 29 \cdot 31$. Then $(p-1)(q-1) = 28 \cdot 30 = 840$. Using the extended Euclidian algorithm, determine that $1 = 3 \cdot 840 - 229 \cdot 11$, so the inverse of 11 mod 840 is $-229 \equiv 611 \pmod{840}$. Now compute $468^{611} \equiv 13 \pmod{899}$ via fast exponentiation. The plaintext is therefore 13. As a check you can compute $13^{11} \equiv 468 \pmod{899}$.

8. We have $m^3 \equiv 208 \pmod{391}$, $m^3 \equiv 38 \pmod{55}$, and $m^3 \equiv 32 \pmod{87}$. As $391 = 17 \cdot 23$, $55 = 55 \cdot 11$ and $87 = 3 \cdot 29$ are all prime, there is a unique solution to this trio of congruences mod $3 \cdot 5 \cdot 11 \cdot 17 \cdot 23 \cdot 29 = 1870935$ by the Chinese Remainder Theorem.

   Let's first solve just the first two congruences. We have $m^3 = 208 + 391x = 38 + 55y$, so $55y - 391x = 170$. Using the extended Euclidian algorithm, we get $y = 64 \cdot 170 = 10880$ and $x = 9 \cdot 170 = 1530$. So $m^3 = 208 + 391 \cdot 1530 = 598438 \equiv 17803 \pmod{391 \cdot 55}$. We could stop here if 17803 were a pure cube as an integer, but unfortunately it isn't. So now we need to solve the pair of congruences $m^3 \equiv 17803 \pmod{391 \cdot 55}$ and $m^3 \equiv 32 \pmod{87}$.

   This gives us $17803 + 21505x = 32 + 87y$, or $87y - 21505x = 17771$. This results in $x = 38 \cdot 17771 = 675298$ and $y = 9393 \cdot 17771 = 166923003$. So $m^3 = 14522301293 \equiv 103823 \pmod{391 \cdot 55 \cdot 87}$. It follows $m = 47$.

   Comments: Most people followed the algorithm in the book for computing using the CRT, which ends up being faster and less effort than doing two steps like this since we didn't get lucky here and find a perfect cube using just one of the steps. Of course either method is perfectly fine.

10. We have $2 \cdot 3 - 1 \cdot 5 = 1$, so given that $m^3 \equiv 293 \pmod{493}$ and $m^5 \equiv 421 \pmod{493}$, we have $m^1 \equiv (m^3)^2 \cdot (m^5)^{-1} \equiv (293)^2 \cdot (421)^{-1} \pmod{493}$. Now $293^2 \equiv 67 \pmod{493}$, and $(421)^{-1} \equiv 89 \pmod{493}$ by the extended Euclidian algorithm. Finally $67 \cdot 89 \equiv 47 \pmod{493}$. As a check, $47^3 \equiv 293 \pmod{493}$ and $47^3 \equiv 293 \pmod{493}$. Hmmm, this message 47 must be very important to have appeared in two different problems!