Math 116
Homework 8 Solutions

I graded 3 of the problems: 14, 16, 18.

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 9. The high score was 9, the median was 7.5 and the mean was 7.4.

14. Since $493 = pq = 17 \cdot 29$, we need to determine the multiplicative order of 3 in $\mathbb{Z}/(p-1)(q-1)\mathbb{Z} = \mathbb{Z}/448\mathbb{Z}$. Now $\phi(448) = \phi(2^6) \cdot \phi(7) = 2^5 \cdot 6 = 192$. So by Fermat's Little Theorem, $3^{192} \equiv 1 \pmod{448}$ but we want to find the order of 3, in other words the smallest positive k such that $3^k \equiv 1 \pmod{448}$. What we know is that k divides $192 = 2^6 \cdot 3$. As $3^{2^6} \equiv 193 \pmod{448}$, we need the factor 3 of 192. We need to try then all $3^{2^m \cdot 3}$ mod 448 for $0 \leq m \leq 6$, and the smallest such m will give us the order $2^m \cdot 3$. We could use binary search at this point. Since $3^{2^3 \cdot 3} \equiv 225 \pmod{448}$, we need to go higher. Since $3^{2^4 \cdot 3} \equiv 1 \pmod{448}$, we're done and $k = 48$.

    Comments: People had trouble with this one, even though we've computing orders of elements in previous homework. I gave one point for realizing you need to compute the order of 3 mod 448 (which almost everyone realized), one point for showing how you would find the order (whether you got it right or not), and one point for the correct answer.

16. Factor $713 = pq = 23 \cdot 31$. Then $\frac{p+1}{4} = 6$ and $\frac{q+1}{4} = 8$. We have $289^6 \equiv 6 \pmod{23}$ and $289^8 \equiv 14 \pmod{31}$. Now $23(-4) + 31(3) = 1$, so let $r = (23)(-4)(8) + (31)(3)(6) \equiv 696 \pmod{713}$ and $s = (23)(-4)(8) + (31)(3)(-6) \equiv 293 \pmod{713}$. Therefore the four possible plaintext messages are $\pm 696 \pmod{713}$ and $\pm 293 \pmod{713}$, or writing them all as positive numbers: $\{696, 17, 293, 420\}$. As a check, square each of these mod 713 and see that it's congruent to 289.

18. Factor $713 = pq = 23 \cdot 31$. Then $\frac{p+1}{4} = 6$ and $\frac{q+1}{4} = 8$. We have $200^6 \equiv 4 \pmod{23}$ and $200^8 \equiv 18 \pmod{31}$. Now $23(-4) + 31(3) = 1$, so let $r = (23)(-4)(18) + (31)(3)(4) \equiv 142 \pmod{713}$ and $s = (23)(-4)(18) + (31)(3)(-4) \equiv 111 \pmod{713}$. Therefore the four possible plaintext messages are $\pm 142 \pmod{713}$ and $\pm 111 \pmod{713}$, or writing them all as positive numbers: $\{142, 571, 111, 602\}$. As a check, square each of these mod 713 and see that it's congruent to 200.

20. As noted in the ammendment to the homework, we need to know A as well, and we will first let $A = 19$. Now Alice knows a such that $g^a \equiv 19 \pmod{43}$, but we don't, so we need to figure it out. Fortunately $p = 43$ is small enough here that we can just use exhaustive search: compute g^a mod 43 for $a = 1, 2, \ldots, 41$ (note that $g^{42} \equiv 1 \pmod{43}$ by Fermat's Little Theorem!) until you get 19. It turns out $a = 19$ works. Now we just need to compute $m = B^{p-1-a}c \bmod p$. With $B = 30$, $p = 43$, $a = 19$ and $c = 7$ we get $30^{23} \cdot 7 \equiv 21 \pmod{43}$. So $m = 21$ is the message.

    As a check, let's encrypt m and make sure we get $c = 7$. We first need to figure out what b is such that $3^b \equiv 30 \pmod{43}$. Again by exhaustive search we get $b = 11$. Then computing $c = A^b m \bmod p$ we get $19^{11} \cdot 21 \equiv 7 \pmod{43}$.

    On the web the value of A given was $A = 25$, so let's try that as well. We need to find a such that $g^a \equiv 25 \pmod{43}$. We again use exhaustive search, and it turns out $a = 8$ works. Now we just need to compute $m = B^{p-1-a}c \bmod p$. With $B = 30$, $p = 43$, $a = 8$ and $c = 7$ we get $30^{34} \cdot 7 \equiv 33 \pmod{43}$. So $m = 33$ is the message.

    As a check, let's encrypt m and make sure we get $c = 7$. As before we have $b = 11$. Then computing $c = A^b m \bmod p$ we get $25^{11} \cdot 33 \equiv 7 \pmod{43}$.