Math 116
Homework 5 Solutions

I graded 4 of the problems: 1, 4, 5 and 2.22.21

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 10, the median was 6 and the mean was 5.9. I graded two computational problems and two proof problems; almost everyone did well on the computations but had trouble with the proofs, so 6 and 7 were the most common scores.

1. Evaluate 2^{12345} mod 691.

   First verify that 691 is prime. Then, by Fermat's little theorem, we know $2^{690} \equiv 1 \pmod{691}$. Using division with remainder we have $12345 = 690 * 17 + 615$, so $2^{12345} \equiv 2^{615} \pmod{691}$. Now use fast exponentiation. By repeated squaring we have

$$\begin{aligned}
2^1 &\equiv 1 \pmod{691} \\
2^2 &\equiv 4 \pmod{691} \\
2^{2^2} &\equiv 16 \pmod{691} \\
2^{2^3} &\equiv 256 \pmod{691} \\
2^{2^4} &\equiv 256^2 \equiv 582 \pmod{691} \\
2^{2^5} &\equiv 582^2 \equiv 134 \pmod{691} \\
2^{2^6} &\equiv 134^2 \equiv 681 \pmod{691} \\
2^{2^7} &\equiv 681^2 \equiv 100 \pmod{691} \\
2^{2^8} &\equiv 681^2 \equiv 326 \pmod{691} \\
2^{2^9} &\equiv 326^2 \equiv 553 \pmod{691}
\end{aligned}$$

   Since $615 = 512 + 64 + 32 + 4 + 2 + 1 = 2^9 + 2^6 + 2^5 + 2^2 + 2 + 1$ we have
   $2^{615} = (2^{2^9})(2^{2^6})(2^{2^5})(2^{2^2})(2^2)(2^1) \equiv 553 \cdot 681 \cdot 134 \cdot 16 \cdot 4 \cdot 2 \equiv 246 \pmod{691}$.

   Comments: Almost everyone got this. I didn't take off for computation errors as long as you showed you understood the method. Most people didn't use Fermat's little theorem but just calculated the full binary expansion of 12345, which uses powers of 2 up to 2^{13}. This is fine as well, and isn't much more work.

2. Find an element of order 442 in $(\mathbb{Z}/443\mathbb{Z})^*$.

   First verify that 443 is prime. Next factor $442 = 2 \cdot 13 \cdot 17$. A good first guess for an element of order 442 is 2. Using Theorem 2.14.1, we compute $2^{13 \cdot 17} \equiv -1 \pmod{443}$, $2^{2 \cdot 17} \equiv 35 \pmod{443}$, and $2^{2 \cdot 13} \equiv 123 \pmod{443}$. This proves that the order of 2 is 442.

3. Find all m such that $(\mathbb{Z}/m\mathbb{Z})^*$ has 4, 6, 8 or 60 elements.

We know that the size of $(\mathbb{Z}/m\mathbb{Z})^*$ is $\phi(m)$ where $\phi(p^n) = p^n - p^{n-1} = p^{n-1}(p-1)$ for p prime, and is multiplicative, meaning that $\phi(k \cdot m) = \phi(k)\phi(m)$ if $\gcd(k, m) = 1$. Let's start computing $\phi(p^n)$ for some small values of p and n.

m	2	2^2	2^3	2^4	3	3^2	5	5^2	7	11	13	31	61
$\phi(m)$	1	2	4	8	2	6	4	20	6	10	12	30	60

No other prime powers will be of use, as you can convince yourself. Not even all of these will be of use, since there are no m such that $\phi(m)$ equals 3 or 5. We now look at all multiplicative combinations to get the possible answers for each group order $\phi(m)$:

$\phi(m)$	m
4	5, 8, 10
6	9, 18
8	10, 15, 16, 24, 30
60	61, 77, 93, 99, 122, 124, 154, 186, 198

4. Find the least positive integer A that is congruent to 7 mod 33, 2 mod 28, and 3 mod 65.

We solve the following congruences:

$$\begin{aligned} y_1(28 \cdot 65) &\equiv 1 \pmod{33} \\ y_2(33 \cdot 65) &\equiv 1 \pmod{28} \\ y_3(33 \cdot 28) &\equiv 1 \pmod{65} \end{aligned}$$

Multiplying and reducing, this gives

$$\begin{aligned} y_1(5) &\equiv 1 \pmod{33} \\ y_2(17) &\equiv 1 \pmod{28} \\ y_3(14) &\equiv 1 \pmod{65} \end{aligned}$$

Using the extended Euclian algorithm or some other method, solutions to these equations are $y_1 = 20$, $y_2 = 5$, and $y_3 = 14$. It follows
$A \equiv 7y_1(28 \cdot 65) + 2y_2(33 \cdot 65) + 3y_3(33 \cdot 28) \equiv 7 \cdot 20 \cdot 28 \cdot 65 + 2 \cdot 5 \cdot 33 \cdot 65 + 3 \cdot 14 \cdot 33 \cdot 28 \equiv 315058 \equiv 14758 \pmod{33 \cdot 28 \cdot 65}$.

Comments: Most people got this right, although I did take off a point if you didn't follow direction and give the least positive answer. Some people calculated an intermediate result using two of the congruences, and then combined that with the final congruence. That's fine as well.

5. Define the nth Fermat Number to be $F_n = 2^{2^n} + 1$. Show that if a prime p divides F_n, then 2^{n+1} divides $p - 1$, i.e., $p \equiv 1 \pmod{2^{n+1}}$. Using this result, show (with only a little computation) that F_4 is prime.

Say that $p | 2^{2^n} + 1$. This means $2^{2^n} \equiv -1 \pmod{p}$. So if we let k be the order of 2 mod p, we know that $k \nmid 2^n$. Squaring both sides of our congruence results in $2^{2^{n+1}} \equiv 1 \pmod{p}$. From this we know that $k \mid 2^{n+1}$. So there is only one possibility, $k = 2^{n+1}$. We also know by Fermat's Little Theorem that $2^{p-1} \equiv 1 \pmod{p}$. Therefore $k = 2^{n+1}$ must divide $p - 1$.

We now use this result to show that $F_4 = 2^{16} + 1$ is prime. Let p be the smallest prime dividing F_4. Then if $p \neq F_4$, we must have $p \leq \sqrt{2^{16} + 1}$ (think about why this must be so). Since $2^{16} + 1$ is just slightly bigger than 2^{16}, it follows $\sqrt{2^{16} + 1}$ is just slightly bigger than $\sqrt{2^{16}} = 2^8 = 256$. In fact if you work it out more precisely you'll see $p \leq 256$. By our result, we also know that $2^5 = 32$ divides $p - 1$, so the only possibilities for p are $p = 33 + 32k$, for $k = 0$ up to $\lfloor \frac{256-33}{32} \rfloor = 6$. So check each of the numbers $33, 65, 97, 129, 161, 193, 225$. Of these, only 97 and 193 are prime, and neither divides F_4, so we're done. Note that you don't have to check if each number is prime or not—you can just blindly divide F_4 by it and make sure there is a non-zero remainder.

Comments: This was a difficult problem and I wasn't going to grade it, but looking over people's assignments I saw most people had attempted a solution, so I was curious to see what everyone wrote. Unfortunately almost all of the solutions were nonsense or just incorrect. Surprisingly almost no one did the work to show F_4 is prime. This was worth 1 point, and the proof 2 points. If you got any points on this problem, think of it as extra credit.

21. Assume $\gcd(a, p) = 1$; otherwise $a \equiv 0 \pmod{p}$ and the problem is trivial. We want to show that $a^{(p+1)/2} \equiv a \pmod{p}$. We have $a \equiv b^2 \pmod{p}$, so $a^{(p+1)/2} \equiv b^{p+1} \pmod{p}$; it is thus enough to show $b^{p+1} \equiv b^2 \pmod{p}$. But $b^{p+1} = b^{p-1}b^2 \equiv b^2 \pmod{p}$ by Fermat's Little Theorem. Note that the condition $p \equiv 3 \pmod{4}$ was only needed so that $(p+1)/4$ would be an integer.

    Comments: I was suprised that almost no one got this one, since it didn't seem very hard. Make sure you understand the solution, at least.

23. In exercise 17 in the last homework we determined that the order of 2 was 1236. It follows the order of $2^{1236/103} = 2^{12}$ is 103.

25. We solve the following congruences:

$$\begin{aligned} y_1(3 \cdot 5 \cdot 7) &\equiv 1 \pmod{2} \\ y_2(2 \cdot 5 \cdot 7) &\equiv 1 \pmod{3} \\ y_3(2 \cdot 3 \cdot 7) &\equiv 1 \pmod{5} \\ y_4(2 \cdot 3 \cdot 5) &\equiv 1 \pmod{7} \end{aligned}$$

    These are easy to solve by inspection. We get $y_1 = 1$, $y_2 = 1$, $y_3 = 3$, and $y_4 = 4$ as solutions. Therefore a solution is

$$1 \cdot 105 + 1 \cdot 70 + 3 \cdot 42 + 4 \cdot 30 = 421 \equiv 1 \pmod{210}.$$

    So we just could have guessed 1 as the answer from the outset, but it's good practice to see how to calculate it using the Chinese Remainder Theorem.