Math 116
Homework 4 Solutions

I graded 4 of the problems: 14, 16, 19

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 7 and the mean was 6.2. I didn't want to grade problem 17, so there were only three problems left and I graded all three of those.

14. To simply prove existence and uniqueness, we can use a proof similar to that done for GCD. Let S be the set of all positive numbers which are common multiples of a and b. Then $|ab|$ is in S, so it is non-empty. Furthermore it is bounded below by definition by 0. Therefore it must have a unique least element, which by definition is the LCM.

    To actually compute the LCM, however, we would like to relate it to the GCD, which we already know how to compute. Once we do this we also get existence and uniqueness. First note that $\operatorname{lcm}(a,b) = \operatorname{lcm}(|a|,|b|)$ and so it suffices to consider only $a, b > 0$. For $a, b > 0$ we first prove that $\operatorname{lcm}(a,b) = \frac{ab}{\gcd(a,b)}$. Once we have this, the rest of the problem follows immediately. Existence and uniqueness of the LCM follows from existence and uniqueness of the GCD, and the LCM can be computed by first computing the GCD using the Euclidean algorithm, and then dividing the product by the GCD.

    Let $\ell = \operatorname{lcm}(a,b)$, let $g = \gcd(a,b)$, and let $m = \frac{ab}{g}$. We want to prove $\ell = m$. Let $a = ga'$ and $b = gb'$ where $\gcd(a',b') = 1$. Now $a|\ell$ and $b|\ell$, so $ga'b'|\ell$. Notice that $ga'b' = m$, so we have $m \leq \ell$. But both a and b divide m, and so m is a common multiple of a and b; by definition it follows $\ell \leq m$. Therefore $\ell = m$.

    Here is another way to look at GCD and LCM which is also interesting. Let $\{p_1, \ldots, p_n\}$ be the set of all primes dividing either a or b and write $a = p_1^{j_1} \cdots p_m^{j_n}$ and $b = p_1^{k_1} \cdots p_m^{k_n}$. The j_i and k_i are determined due to unique factorization, but here some of them may be 0.

    Using these factorizations, we have

$$\begin{aligned} ab &= p_1^{j_1+k_1} \cdots p_n^{j_n+k_n} \\ \gcd(a,b) &= p_1^{\min(j_1,k_1)} \cdots p_n^{\min(j_n,k_n)} \\ \operatorname{lcm}(a,b) &= p_1^{\max(j_1,k_1)} \cdots p_n^{\max(j_n,k_n)} \end{aligned}$$

    and it is easy to see that $\operatorname{lcm}(a,b) = \frac{ab}{\gcd(a,b)}$ follows from this.

    Comments: Most people used the first proof to show existence and uniqueness, although many neglected to show that S is nonempty. Also most people at least stated the relationship between LCM and GCD, but very few were able to prove it.

16. Computing mod 17, we have $2 \to 4 \to 8 \to 16 \to 15 \to 13 \to 9 \to 1$ (where each step we multiply by 2), so the group is $\{1, 2, 4, 8, 9, 13, 15, 16\}$, a cyclic group of order 8.

    Comments: Almost everyone had no trouble with this problem.

17. By Fermat's Little Theorem, $2^{1236} \equiv 1 \pmod{1237}$. Therefore the smallest positive x such that $2^x \equiv 1 \pmod{1237}$ must divide $1236 = 2^2 \cdot 3 \cdot 103$. Therefore you can try out each proper divisor d of 1236 and compute $2^d \pmod{1237}$ to see that it is not 1. It follows the order of 2 mod 1237 is 1236. If you didn't want to use Fermat's Little Theorem you could have also just computed every $2^n \pmod{1237}$ starting from $n = 1$ and stopped when you reached 1 (which would of course be at $n = 1236$). Writing a computer program to do this would help.

19. By Fermat's Little Theorem, $2^6 \equiv 1 \pmod 7$. Therefore $2^{20} = (2^6)^3 \cdot 2^2 \equiv 1^3 \cdot 4 \equiv 4 \pmod 7$.

    Another way to solve this is to peek ahead to section 12 and use fast exponentiation. We have $20 = 2^4 + 2^2$, so $2^{20} = 2^{2^4} \cdot 2^{2^2}$. Using repeated squaring, we have $2^2 \equiv 4 \pmod 7$, $2^{2^2} = (2^2)^2 = 4^2 = 16 \equiv 2 \pmod 7$, $2^{2^3} = (2^{2^2})^2 \equiv 2^2 \equiv 4 \pmod 7$, and $2^{2^4} = (2^{2^3})^2 \equiv 4^2 \equiv 2 \pmod 7$. Therefore $2^{20} = 2^{2^4} \cdot 2^{2^2} \equiv 2 \cdot 2 \equiv 4 \pmod 7$.

    Comments: Some people just did this by brute force, and although I gave full credit you should make sure to learn the efficient methods.