Math 116
Homework 1 Solutions

I graded 4 of the problems:
Section 1.12: 4, 8, 12; plus webpage problem E.

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 9 and the mean was 7.9. I graded two easier computational problems and two harder proof problems. As this was the first assignment I was fairly generous in grading; in particular I did not take off for sketchy and poorly-written proofs. However I will be much more strict about this from now on. Please write clear proofs and be generous with words to explain what you're doing!

2. The only divisors of 2^n are $\pm 1, \pm 2, \pm 2^2, \ldots, \pm 2^n$, so there are $2n+2$ divisors. Note that this is correct in the boundary case $n = 0$.

4. Following the proof in the book somewhat, if $-b/2 < r \leq b/2$, then dividing all sides of the latter by b we have $-1/2 < r/b \leq 1/2$. Now if $a = qb + r$ is also to hold, we must have $-1/2 < a/b - q \leq 1/2$, which implies $1/2 > q - a/b \geq -1/2$ which implies $a/b - 1/2 \leq q < a/b + 1/2$. It is always possible to find an integer in the interval $[\frac{a}{b} - \frac{1}{2}, \frac{a}{b} + \frac{1}{2})$, so this is our q and we've proven existence. In fact there is exactly one integer in this interval so we've proven uniqueness as well: Once q is determined this way then $r = q - qb$. We can specify the value of q as $\lceil \frac{a}{b} - \frac{1}{2} \rceil$.

   Some people said $q = \lfloor \frac{a}{b} + \frac{1}{2} \rfloor$, but note that that would lie in the range $(\frac{a}{b} - \frac{1}{2}, \frac{a}{b} + \frac{1}{2}]$ This is a subtle point, though, and I didn't otherwise take off for it.

   Some people followed a different proof which was based on one done in class. Let $S = \{a - qb : q \in \mathbb{Z} \text{ and } a - qb > -b/2\}$. Since this is a set of integers with a lower bound, it must have a least element, call it r_0. By definition there is some $q_0 \in \mathbb{Z}$ such that $a - q_0 b = r_0$; also by definition $-b/2 < r_0$. We claim also that $r_0 \leq b/2$. $r_0 > b/2$ then $a - (q_0 + 1)b = r_0 - b > -b/2$, and so $r_0 - b \in S$ which contradicts minimality of r_0 (note that $b > 0$). This proves existence.

   One can then prove uniqueness as follows. Pretend there are two pairs q, r and q', r' with $-1/2 < r, r' \leq 1/2$ that satisfy $a = qb + r$ and $a = q'b + r'$, Then we have $qb + r = q'b + r'$ and so $(q - q')b = r' - r$. However $-1 < \frac{r'-r}{b} < 1$, which implies $-1 < q - q' < 1$, and since both q and q' are integers we must have $q' - q = 0$ and therefore $r - r' = 0$; it follows $q = q'$ and $r = r'$.

6. Clearly the integer 1 satisfies all three congruences. A general method for solving simultaneous congruences is given in Section 2.15 on the Chinese Remainder Theorem. ("Chinese Remainder Theorem" is missing from the index, so I was worried for a while that it wasn't covered in the book, which would be very strange given its fundamental importance for both number theory and cryptography.)

8. The number 2^m ($m \geq 0$) has binary length $m + 1$, and as long as $m > 0$ then $2^m + 1$ has the same length. In the case $m = 2^n$, where $n \geq 0$, it follows $m > 0$ and so $2^{2^n} + 1$ has binary length $2^n + 1$.

   Comments: If you wrote down the correct answer without a decent justification, I gave only two points. Almost no one discussed the boundary case; be sure to be careful about this in the future. Most people used Theorem 1.3.3, but were not careful about evaluating $\lfloor \log_2 2^{2^n} + 1 \rfloor + 1$. However I was fairly generous grading this.

12. Since $f = O(F)$ we know there exist positive integers B_1, C_1 such that $f(n_1, \ldots, n_k) \leq C_1 F(n_1, \ldots, n_k)$ for all $n_i \geq B_1$, $1 \leq i \leq k$. Similarly since $g = O(G)$ we know there exist positive integers B_2, C_2 such that $g(n_1, \ldots, n_k) \leq C_2 G(n_1, \ldots, n_k)$ for all $n_i \geq B_2$, $1 \leq i \leq k$. Let $B = \max(B_1, B_2)$ and $C = \max(C_1, C_2)$, and it follows that $(f+g)(n_1, \ldots, n_k) = f(n_1, \ldots, n_k) + g(n_1, \ldots, n_k) \leq CF(n_1, \ldots, n_k) + CG(n_1, \ldots, n_k) = C(F+G)(n_1, \ldots, n_k)$ for all $n_i \geq B_1$, $1 \leq i \leq k$, and therefore $f + g = O(F + G)$. Let $C' = C_1 \cdot C_2$ and it follows similarly that that $fg = O(FG)$ using B, C' as the constants.

    Comments: Almost no one handled the B_i constants in their solutions, but I didn't take off for this.

C. $[10000]_{10} = [10011100010000]_2 = [111201101]_3 = [41104]_7$.

D. $[3421]_5 + [1234]_5 = [10210]_5$. $[3421]_5 \cdot [1234]_5 = [11004114]_5$. $[101010]_2 = [110]_2 \cdot [111]_2 + [0]_2$.

E. Answer: BE01.

    Comments: Almost everyone got this right. I took off one point for each hexidecimal digit wrong.