Math 116
Homework 2 Solutions

I graded 3 of the problems:
Section 1.12: 14, 16, 22.

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 7, the median was 5 and the mean was 4.7. There were only three problems to grade so of course I picked those three! As I mentioned in the comments for the last homework, I am being much stricter in grading proofs starting from this assignment. Be sure to write your proofs carefully and in detail, using full sentences and explain clearly what you're doing.

14 Let's follow the proof of Theorem 1.8.3 and see what changes we need to make. We again define the series of remainders r_i for $i \geq 0$ where $r_0 = |a|$, $r_1 = |b|$, and r_{k+1} is the unique integer in $(-|r_k|/2, |r_k|/2]$ such that $r_{k-1} = q \cdot r_k + r_{k+1}$ for some $q \in \mathbb{Z}$ (which is also unique). This all follows from problem 4 which was on the last assignment.

Note that we no longer have $r_{k+1} = r_{k-1} \bmod r_k$ since by the book's definition of mod, r_{k+1} would have to lie in $[0, |r_k|)$. So we can't just invoke Theorem 1.8.1. We can however prove directly the result we need, namely that $\gcd(r_{k-1}, r_k) = \gcd(r_k, r_{k+1})$. This follows from the equation $r_{k-1} = q \cdot r_k + r_{k+1}$. If d is any divisor of both r_k and r_{k+1}, then it must also divide r_{k-1}. Therefore $\gcd(r_k, r_{k+1})$ divides r_{k-1}. It also divides r_k and therefore $\gcd(r_k, r_{k+1})$ divides $\gcd(r_k, r_{k-1})$.

We also have $r_{k-1} - q \cdot r_k = r_{k+1}$, and so if d is any divisor of both r_k and r_{k-1}, then it must also divide r_{k_1}. Therefore $\gcd(r_k, r_{k-1})$ divides r_{k+1}. It also divides r_k and therefore $\gcd(r_k, r_{k-1})$ divides $\gcd(r_k, r_{k+1})$. So each divides the other, and since both are positive they must be equal.

Finally we must show that the algorithm terminates. This follows because $-r_k/2 < r_{k+1} \leq r_k/2$ and so $|r_{k+1}| < |r_k|$; also all the $r_k \in \mathbb{Z}$ of course. The algorithm terminates when $|r_k| = 0$.

Comments: Solutions for this problem were uniformly bad; I didn't give more than one point to anyone for this problem. In the future I expect to see proofs written out clearly, explained well and in detail.

16 We use our new division algorithm in which the remainder is in the range $(-b/2, b/2]$.

$$\begin{aligned} 235 &= 2 \cdot 124 - 13 \\ 124 &= 10 \cdot 13 - 6 \\ 13 &= 2 \cdot 6 + 1 \\ 6 &= 6 \cdot 1. \end{aligned}$$

This gives $\gcd(235, 124) = 1$ as before. Using back substitution to compute the representation of the gcd, we get

$$\begin{aligned} 1 &= 13 - 2 \cdot 6 \\ &= 13 - 2(124 - 10 \cdot 13) \\ &= -19 \cdot 13 + 2 \cdot 124 \\ &= -19(-235 + 2 \cdot 124) + 2 \cdot 124 \\ &= 19 \cdot 235 - 36 \cdot 124 \end{aligned}$$

and so the representation is also the same as before. When computing the representation it's a good idea to check every line to make sure you still have equality; this will help catch mistakes before things get out of control.

Notice that the modified algorithm found the gcd faster than the original algorithm did. The reason is that the absolute value of the remainder is forced to be smaller than in the original algorithm. Note however that there are examples in which the modified and original algorithms would take the same number of steps.

Comments: Some people just repeated the solution to problem 15; I gave no credit for that. A lot of people forgot to compute the representation, but I took off only one point for omitting that.

22 We start by noting that $37800 = 378 \cdot 100 = (189 \cdot 2) \cdot (2 \cdot 2 \cdot 5 \cdot 5)$. Now 7 divides 189, the quotient being 27, so our final factorization is $2^3 \cdot 3^3 \cdot 5^2 \cdot 7$.