Math 113(4) - Comments for HW1

Seewoo Lee

September 3, 2018

Some general comments:

1. Please use staplers or clips, not just fold the left-upper corner of papers!
2. Try to write well! - maybe this will be harder than the first one...
3. If you can, try to use LaTeX.
4. For questions that requires proofs, I almost not give any partial credits.

Problem 1

There are many people who only shows $\gcd(a,b) \mid \gcd(b,r)$, and I only give 2.5 points for them. You should show both $\gcd(a,b) \mid \gcd(b,r)$ and $\gcd(b,r) \mid \gcd(a,b)$, for the full credit.

Problem 2

2.5 points for each a) and b). If approach is right but you did some mistakes, I deducted 0.5 points for each problem. If you did well but write the answer of a) as 14, I gave only 1 point.

Problem 3

I gave full credits who used the unique factorization of integers (which is also called the *fundamental theorem of arithemetic*). Also, you may use proof by contradiction: if $p \nmid a$ and $p \nmid b$, then $px + ay = 1$ and $px' + by' = 1$, and you can find $x'', y'' \in \mathbb{Z}$ so that $px'' + aby'' = 1$.

Some people use the following argument: if $p \nmid a$ and $p \nmid b$, by division algorithm, we can find q, r, q', r' s.t. $0 < r, r' < p$ and $a = pq + r, b = pq' + r'$. Then $ab = p(pqq' + qr' + q'r) + rr'$ - and this is not a multiple of p since both r and r' aren't. This is a wrong proof, since the last argument requires the original lemma we are going to prove, which is a circular logic.

Problem 4

The most crucial part of the proof is to show $a \equiv a' \pmod{n}$ and $b \equiv b' \pmod{n}$ implies $a + a' \equiv b + b' \pmod{n}$, which is the only thing that requires. You may think that this is trivial, but you have to *show* this. I don't give any point if you didn't show this.