Assignment **HW 6**

---

Solutions by **Ayawa Xing** `awx856(at)u.e.`

This document contains my solutions to the Gradescope assignment named on the top of this page. Specifically, my solutions to the following problems are included:

- 4.12 (a)(c) (page 2)
- 4.13 (a)(b)(c) (pages 3–5)
- 4.17 (a)(b) (page 6)

I did not forget

- to REFRESH my browser for the latest information about each problem
- to link problems to pages.
  This page is linked to the problems I did not solve.
- to update the items marked *** in the template (my name, email, the Gradescope title of the assignment, the list of problems solved, the `\lhead` statements (left page headers: list of (sub)problems solved on each page)
- to make sure no subproblem solution spills over to the next page (except when this is unavoidable, i.e., when the solution to a subproblem does not fit on a page)
- if a problem takes more than one page, I linked each of those pages to the problem
- I took care not to defeat the mechanisms provided by this template.

With each problem, **I stated my sources and collaborations**.
By submitting this solution *I certify* that *my statement of sources and collaborations is accurate and complete.* I understand that without this certification, my solutions will not be accepted.
In case I am giving a link to a source, *I am also sending this link to the instructor by email.*

4.12(a) Question.
Prove the identity

$$\sum_{k=0}^{n} \binom{n}{k}^2 = \binom{2n}{n} \tag{1}$$

*Sources and collaborations.*
Marny Dillon suggested to look up “Vandermonde’s Identity.”
in Wikipedia

*Answer.*
(your proof here) □

---

4.12 (c) Question.
Prove that in a tree, all longest paths share a vertex.

*Sources and collaborations.* I found this at
`http://hpca23.cse.wamu.edu/weevil/~jhl/discretebook/chap4.pdf/`

*Answer.*
(your proof here) □

4.13 (a) Question.
Let $a \in \mathbb{Z}$. Let $x = 3a - 5$ and $y = 7a - 8$. Prove: $\gcd(x, y)$ is either 1 or 11.

*Sources and collaborations.* Discussed with Marny Dillon. We figured this out together.

*Answer.*
Let $d = \gcd(x, y)$. Then $d \mid 3y - 7x = 11$. Since 11 is a prime, its only positive divisors are 1 and 11. $\square$

---

4.13(b) Question.
Find a value of $a$ such that $\gcd(x, y) = 11$.

*Sources and collaborations.* Discussed with Marny Dillon. Marny simplified my more complicated idea. Marny suggested the idea of the general solution; I worked out the details by myself.

*Answer.*
Take $a = 9$. Then $x = 22$ and $y = 55$, so $\gcd(x, y) = 11$. $\square$

Comment. The general solution is

$$\gcd(x, y) = 11 \iff a \equiv -2 \pmod{11}.$$

*Proof.* Since $3x - 7y = 11$, we have that $11 \mid x \iff 11 \mid y$. So $\gcd(x, y) = 11 \iff 11 \mid x \iff 11 \mid 3a - 5 \iff 3a \equiv 5 \pmod{11}$. Multiplying both sides by 4 which is relatively prime to 11 we see that $3a \equiv 5 \pmod{11} \iff 12a \equiv 20 \pmod{11}$. But $12a \equiv a \pmod{11}$ and $20 \equiv -2 \pmod{11}$. $\square$

4.13(c) Question.
For what values $a$ and $b$ is it the case that

$$\gcd(a+b, a-b) = \gcd(a,b) \quad ?$$

*Sources and collaborations.* None.

*Answer.*
For an integer $x$, let $\ell(x)$ denote the largest $k$ such that $2^k \mid x$. If no largest $k$ exists, we write $\ell(x) = \infty$. For instance, $\ell(12) = 2$ and $\ell(9) = 0$ and $\ell(0) = \infty$.

**Claim.** $\gcd(a+b, a-b) = \gcd(a,b)$ if and only if either $a = b = 0$ or $\ell(a) \neq \ell(b)$.

*Proof.* If $\gcd(a,b) = 0$ then $a = b = 0$ and therefore both sides of the "if and only if" statement are true: $\gcd(a+b, a-b) = \gcd(0,0) = \gcd(a,b)$, and $a = b = 0$.

Assume now that $a = 0$ and $b \neq 0$. In this case again both sides of the "if and only if" statement are true: $\gcd(a,b) = |b| = \gcd(a+b, a-b)$, and $\ell(a) \neq \ell(b)$ because $\ell(a) = \infty$ and $\ell(b)$ is finite.

This also settles the case when $a \neq 0$ and $b = 0$ (by switching the roles of $a$ and $b$).

Henceforth we assume that $a \neq 0$ and $b \neq 0$.
In particular, $\gcd(a,b) \neq 0$.

First we prove the **"only if" direction.** In this part, we have:
**Assumption:** $\gcd(a+b, a-b) = \gcd(a,b)$.
**Desired conclusion:** $\ell(a) \neq \ell(b)$.
*Proof* by contradiction. Assume for a contradiction that $\ell(a) = \ell(b) =: k$. Let $a' = a/2^k$ and $b' = b/2^k$. Then $\gcd(a,b) = \gcd(2^k a', 2^k b') = 2^k \gcd(a', b')$ and similarly $\gcd(a+b, a-b) = 2^k \gcd(a'+b', a'-b')$. So our assumption is equivalent to saying that $\gcd(a'+b', a'-b') = \gcd(a', b')$.

But now both $a'$ and $b'$ are odd, therefore $\gcd(a'b')$ is odd and $\gcd(a'+b', a'-b')$ is even (because both $a'+b'$ and $a'-b'$ are even), a contradiction with the assumption that $\gcd(a'+b', a'-b') = \gcd(a', b')$. This contradiction completes the proof of the "only if" direction. $\square$

Now we prove the **"if" direction.** In this part, we have:
**Assumption:** $\ell(a) \neq \ell(b)$.
**Desired conclusion:** $\gcd(a+b, a-b) = \gcd(a,b)$.

We proceed by first proving a pair of Lemma and a Corollary.

**Lemma 1.** For all $a$ and $b$ we have $\gcd(a,b) \mid \gcd(a+b, a-b)$.
(Note: "for all $a$ and $b$" includes the cases when $a$ or $b$ is zero.)
*Proof.* Let $d \mid a$ and $d \mid b$. Then (by the additivity of divisibility) we have $d \mid a+b$ and $d \mid a-b$, and therefore, $d \mid \gcd(a+b, a-b)$. □

**Lemma 2.** For all $a$ and $b$ we have $\gcd(a+b, a-b) \mid 2 \cdot \gcd(a,b)$.
*Proof.* Let $D \mid a+b$ and $D \mid a-b$. Then (again by the additivity of divisibility) we have $D \mid (a+b)+(a-b) = 2a$ and $d \mid (a+b)-(a-b) = 2b$, and therefore, $D \mid \gcd(2a, 2b) = 2\gcd(a,b)$, proving Lemma 2. □

Corollary. For all $a$ and $b$, the value of $\gcd(a+b, a-b)$ is either equal to $\gcd(a,b)$ or to $2 \cdot \gcd(a,b)$.

First consider the case $\gcd(a,b) = 0$. In this case $a = b = 0$ and therefore $\gcd(a+b, a-b) = \gcd(0,0) = 0$.

Assume now that $\gcd(a,b) \neq 0$. By Lemma 1, there exists an integer $x$ such that $\gcd(a+b, a-b) = x \cdot \gcd(a,b)$. So by Lemma 2, $x \cdot \gcd(a,b) \mid 2 \cdot \gcd(a,b)$. Since $\gcd(a,b) \neq 0$, we conclude that $x \mid 2$ and therefore $x = \pm 1$ or $x = \pm 2$. Since $x \geq 0$ (because every gcd is by definition $\geq 0$), we conclude that $x = 1$ or 2, completing the proof of the Corollary. □

Now back to the **proof of the "if" direction.** We continue to assume that $a \neq 0$ and $b \neq 0$.
WLOG (without loss of generality) we may assume that $\ell(a) < \ell(b)$. Let $k = \ell(a)$ and let $a' = a/2^k$ and $b' = b/2^k$. Now $a'$ is odd and $b'$ is even.

As before, we have $\gcd(a,b) = 2^k \gcd(a'b')$ and $\gcd(a+b, a-b) = 2^k \gcd(a'+b', a'-b')$. So to prove our desired conclusion, it suffices to prove that $\gcd(a'+b', a'-b') = \gcd(a', b')$.
Proof by contradiction. Assume $\gcd(a'+b', a'-b') \neq \gcd(a', b')$. Then, by the Corollary, $\gcd(a'+b', a'-b') = 2 \cdot \gcd(a', b')$. This means $\gcd(a'+b', a'-b')$ is even. But this is impossible because now both $a'+b'$ and $a'-b'$ are odd. This contradiction completes the proof of the Claim. □

4.17 (a) Question.
Assume $589 \nmid a$. Does it follow that $a^{588} \equiv 1 \pmod{589}$ ?

*Sources and collaborations.* None.

*Answer.*
No. Counterexample: $a = 19$. Proof by contradiction. First we observe that $589 \nmid 19$. Now suppose for a contradiction that $19^{588} \equiv 1 \pmod{589}$. Then $19^{588} \equiv 1 \pmod{19}$ because $19 \mid 589$. On the other hand, $19^{588} \equiv 0 \pmod{19}$ and therefore $1 \equiv 0 \pmod{19}$, a contradiction. $\square$

---

4.17 (b) Question.
Assume $\gcd(a, 589) = 1$. Prove: $a^{90} \equiv 1 \pmod{589}$.

*Sources and collaborations.* I found a similar problem in Abramov's "Elementary exercises in number theory," Problem 2.17,
`http://kvabramov.org/numbook/chap2.pdf`

*Answer.*
$589 = 19 \cdot 31$ and both 19 and 31 are primes. In particular, they are relatively prime; therefore it suffices to prove that

(i) $a^{90} \equiv 1 \pmod{19}$ and
(ii) $a^{90} \equiv 1 \pmod{31}$.

We know that $\gcd(a, 19) = 1$ and $\gcd(a, 31) = 1$. Therefore, by Fermat's little theorem, we have

$$a^{18} \equiv 1 \pmod{19} \tag{2}$$

and

$$a^{30} \equiv 1 \pmod{31} \tag{3}$$

Raising both sides of Eq. (2) to the fifth power we get item (i), and similarly, raising both sides of Eq. (3) to the third power we obtain item (ii). $\square$