University of Minnesota, School of Mathematics

Math 4281: Introduction to Modern Algebra, Spring 2019: Homework 2

Darij Grinberg

May 27, 2019

1 Exercise 1: gcd basics

1.1 Problem

Prove the following:

(a) If a_1, a_2, b_1, b_2 are integers satisfying $a_1 \mid b_1$ and $a_2 \mid b_2$, then $\gcd(a_1, a_2) \mid \gcd(b_1, b_2)$.

(b) If a, b, c, s are integers, then $\gcd(sa, sb, sc) = |s| \gcd(a, b, c)$.

1.2 Solution

(a) See the class notes, where this is Exercise 2.9.4. (The numbering may shift; it is one of the exercises in the "Common divisors, the Euclidean algorithm and the Bezout theorem" section.)

(b) See the class notes, where this is Exercise 2.9.6. (The numbering may shift; it is one of the exercises in the "Common divisors, the Euclidean algorithm and the Bezout theorem" section.)

2 Exercise 2: Products of gcds

2.1 Problem

Prove the following:

Any four integers u, v, x, y satisfy $\gcd(u, v) \gcd(x, y) = \gcd(ux, uy, vx, vy)$.

2.2 Solution

See the class notes, where this is Exercise 2.10.10. (The numbering may shift; it is one of the exercises in the "Coprime integers" section.)

---

3 Exercise 3: The gcd-lcm connection for three numbers

3.1 Problem

Let a, b, c be three integers. Prove that $\operatorname{lcm}(a, b, c) \gcd(bc, ca, ab) = |abc|$.

3.2 Solution

See the class notes, where this is Exercise 2.11.2 **(b)**. (The numbering may shift; it is one of the exercises in the "Lowest common multiples" section.)

---

4 Exercise 4: Divisibility tests for $3, 9, 11, 7$

4.1 Problem

Let n be a positive integer. Let "$d_k d_{k-1} \cdots d_0$" be the decimal representation of n; this means that $d_0, d_1, \ldots, d_k$ are digits (i.e., elements of $\{0, 1, \ldots, 9\}$) such that $n = d_k 10^k + d_{k-1} 10^{k-1} + \cdots + d_0 10^0$. The digits $d_0, d_1, \ldots, d_k$ are called the *digits of* n.

(Incidentally, the quickest way to find these digits is by repeated division with remainder: To obtain the decimal representation of $n \geq 10$, you take the decimal representation of $n//10$ and append the digit $n\%10$ at the end. Thus,

$$d_0 = n\%10, \qquad d_1 = (n//10)\%10, \qquad d_2 = ((n//10)//10)\%10, \qquad \text{etc.}$$

But in this exercise, you can just assume that the decimal representation exists.)

(a) Prove that $3 \mid n$ if and only if $3 \mid d_k + d_{k-1} + \cdots + d_0$. (In other words, a positive integer n is divisible by 3 if and only if the sum of its digits is divisible by 3.)

(b) Prove that $9 \mid n$ if and only if $9 \mid d_k + d_{k-1} + \cdots + d_0$. (In other words, a positive integer n is divisible by 9 if and only if the sum of its digits is divisible by 9.)

(c) Prove that $11 \mid n$ if and only if $11 \mid (-1)^k d_k + (-1)^{k-1} d_{k-1} + \cdots + (-1)^0 d_0$. (In other words, a positive integer n is divisible by 11 if and only if the sum of its digits in the even positions minus the sum of its digits in the odd positions is divisible by 11.)

(d) Let $q = d_k 10^{k-1} + d_{k-1} 10^{k-2} + \cdots + d_1 10^0$. (Equivalently, $q = n//10 = \dfrac{n - d_0}{10}$; this is the number obtained from n by dropping the least significant digit.) Prove that $7 \mid n$ if and only if $7 \mid q - 2d_0$.

(This gives a recursive test for divisibility by 7.)

4.2 Solution sketch

We will use the following quasi-trivial lemma:

Lemma 4.1. *Let n, x, y be three integers such that $x \equiv y \bmod n$. Then, we have $n \mid x$ if and only if $n \mid y$.*

Proof of Lemma 4.1. $\Longrightarrow$: Assume that $n \mid x$. We must prove that $n \mid y$.

We have $n \mid x$, thus $x \equiv 0 \bmod n$. But $x \equiv y \bmod n$ and thus $y \equiv x \equiv 0 \bmod n$. Hence, $n \mid y$. This proves the "$\Longrightarrow$" direction of Lemma 4.1.

$\Longleftarrow$: Assume that $n \mid y$. We must prove that $n \mid x$.

We have $n \mid y$, thus $y \equiv 0 \bmod n$. But $x \equiv y \equiv 0 \bmod n$. Hence, $n \mid x$. This proves the "$\Longleftarrow$" direction of Lemma 4.1. □

(a) We have $10 \equiv 1 \bmod 3$. Thus, each $m \in \mathbb{N}$ satisfies

$$10^m \equiv 1^m = 1 \bmod 3. \tag{1}$$

Now,

$$\begin{aligned} n &= d_k \underbrace{10^k}_{\substack{\equiv 1 \bmod 3 \\ \text{(by (1))}}} + d_{k-1} \underbrace{10^{k-1}}_{\substack{\equiv 1 \bmod 3 \\ \text{(by (1))}}} + \cdots + d_0 \underbrace{10^0}_{\substack{\equiv 1 \bmod 3 \\ \text{(by (1))}}} \\ &\equiv d_k + d_{k-1} + \cdots + d_0 \bmod 3. \end{aligned}$$

Thus, $3 \mid n$ if and only if $3 \mid d_k + d_{k-1} + \cdots + d_0$ (by Lemma 4.1, applied to 3, n and $d_k + d_{k-1} + \cdots + d_0$ instead of n, x and y).

This solves part **(a)**.

(b) The solution to part **(b)** is precisely the same as that for part **(a)**, except that the 3's need to be replaced by 9's.

(c) We have $10 \equiv -1 \bmod 11$. Hence, each $m \in \mathbb{N}$ satisfies

$$10^m \equiv (-1)^m \bmod 11. \tag{2}$$

Now,

$$\begin{aligned} n &= d_k \underbrace{10^k}_{\substack{\equiv (-1)^k \bmod 11 \\ \text{(by (2))}}} + d_{k-1} \underbrace{10^{k-1}}_{\substack{\equiv (-1)^{k-1} \bmod 11 \\ \text{(by (2))}}} + \cdots + d_0 \underbrace{10^0}_{\substack{\equiv (-1)^0 \bmod 11 \\ \text{(by (2))}}} \\ &\equiv d_k (-1)^k + d_{k-1} (-1)^{k-1} + \cdots + d_0 (-1)^0 \\ &= (-1)^k d_k + (-1)^{k-1} d_{k-1} + \cdots + (-1)^0 d_0 \bmod 11. \end{aligned}$$

Thus, $11 \mid n$ if and only if $11 \mid (-1)^k d_k + (-1)^{k-1} d_{k-1} + \cdots + (-1)^0 d_0$ (by Lemma 4.1, applied to 11, n and $(-1)^k d_k + (-1)^{k-1} d_{k-1} + \cdots + (-1)^0 d_0$ instead of n, x and y). This solves part **(c)**.

(d) We have

$$\begin{aligned} n &= d_k 10^k + d_{k-1} 10^{k-1} + \cdots + d_0 10^0 \\ &= \underbrace{\left(d_k 10^k + d_{k-1} 10^{k-1} + \cdots + d_1 10^1\right)}_{=10 \cdot \left(d_k 10^{k-1} + d_{k-1} 10^{k-2} + \cdots + d_1 10^0\right)} + d_0 \underbrace{10^0}_{=1} \\ &= 10 \cdot \underbrace{\left(d_k 10^{k-1} + d_{k-1} 10^{k-2} + \cdots + d_1 10^0\right)}_{=q} + d_0 = 10q + d_0. \end{aligned}$$

Now, we need to prove two claims:

Claim 1: If $7 \mid n$, then $7 \mid q - 2d_0$.

Claim 2: If $7 \mid q - 2d_0$, then $7 \mid n$.

Proof of Claim 1: Assume that $7 \mid n$. Then, $7 \mid n = 10q + d_0 = d_0 - (-10q)$, so that $d_0 \equiv -10q \bmod 7$. Hence,

$$q - 2 \underbrace{d_0}_{\equiv -10q \bmod 7} \equiv q - 2(-10q) = \underbrace{21}_{\equiv 0 \bmod 7} q \equiv 0 \bmod 7,$$

so that $7 \mid q - 2d_0$. This proves Claim 1.

Proof of Claim 2: Assume that $7 \mid q - 2d_0$. Thus, $q \equiv 2d_0 \bmod 7$. Hence,

$$n = 10 \underbrace{q}_{\equiv 2d_0 \bmod 7} + d_0 \equiv 10(2d_0) + d_0 = \underbrace{21}_{\equiv 0 \bmod 7} d_0 \equiv 0 \bmod 7,$$

so that $7 \mid n$. This proves Claim 2.

Now, part **(d)** of the problem is solved.

---

5 Exercise 5: A divisibility

5.1 Problem

Let $n \in \mathbb{N}$. Prove that $7 \mid 3^{2n+1} + 2^{n+2}$.

5.2 Solution

See the class notes, where this is Exercise 2.5.1. (The numbering may shift; it is one of the exercises in the "Substitutivity for congruences" section.)

6 Exercise 6: A binomial coefficient sum

6.1 Problem

Let $n \in \mathbb{N}$. Prove that

$$\sum_{k=0}^{n} \binom{-2}{k} = (-1)^n \left((n+2) // 2\right). \qquad (3)$$

6.2 Solution

Recall the following fact (which was the claim of Exercise 3 **(d)** on homework set #0):

Proposition 6.1. *Any $n \in \mathbb{Q}$ and $k \in \mathbb{Q}$ satisfy*

$$\binom{-n}{k} = (-1)^k \binom{k+n-1}{k}.$$

Let us also recall another fact (the claim of Exercise 3 **(c)** on homework set #0):

Proposition 6.2. *If $n \in \mathbb{N}$ and $k \in \mathbb{Q}$, then*

$$\binom{n}{k} = \binom{n}{n-k}.$$

Next, we show a simple formula for the binomial coefficients in the exercise:

Lemma 6.3. *If $k \in \mathbb{N}$, then*

$$\binom{-2}{k} = (-1)^k (k+1).$$

Proof of Lemma 6.3. Let $k \in \mathbb{N}$. Then, Proposition 6.1 (applied to 2 instead of n) yields

$$\binom{-2}{k} = (-1)^k \binom{k+2-1}{k} = (-1)^k \binom{k+1}{k} \qquad (4)$$

(since $k+2-1 = k+1$). But $k \in \mathbb{N}$ and thus $k+1 \in \mathbb{N}$. Hence, Proposition 6.2 (applied to $k+1$ instead of n) yields

$$\begin{aligned}
\binom{k+1}{k} &= \binom{k+1}{(k+1)-k} = \binom{k+1}{1} \qquad (\text{since } (k+1)-k = 1) \\
&= \frac{(k+1)\left((k+1)-1\right)\left((k+1)-2\right)\cdots\left((k+1)-1+1\right)}{1!} \\
&\qquad \left(\text{by the definition of } \binom{k+1}{1}\right) \\
&= \frac{k+1}{1!} \qquad \left(\begin{array}{c}\text{since the} \\ \text{product } (k+1)\left((k+1)-1\right)\left((k+1)-2\right)\cdots\left((k+1)-1+1\right) \\ \text{has only one factor}\end{array}\right) \\
&= \frac{k+1}{1} = k+1.
\end{aligned}$$

Hence, (4) becomes

$$\binom{-2}{k} = (-1)^k \underbrace{\binom{k+1}{k}}_{=k+1} = (-1)^k (k+1).$$

This proves Lemma 6.3. ☐

Now, in order to solve the problem at hand, it suffices to prove the identity

$$\sum_{k=0}^{n} (-1)^k (k+1) = (-1)^n ((n+2)//2). \tag{5}$$

Indeed, once (5) is proven, it will follow that

$$\sum_{k=0}^{n} \underbrace{\binom{-2}{k}}_{\substack{=(-1)^k(k+1) \\ \text{(by Lemma 6.3)}}} = \sum_{k=0}^{n} (-1)^k (k+1) = (-1)^n ((n+2)//2)$$

(by (5)), and thus the exercise will be solved.

Before we prove (5), let us state some basic facts about even and odd numbers:

Proposition 6.4. *Let u be an integer.*

(a) *The integer u is even if and only if $u\%2 = 0$.*
(b) *The integer u is odd if and only if $u\%2 = 1$.*
(c) *The integer u is even if and only if $u \equiv 0 \mod 2$.*
(d) *The integer u is odd if and only if $u \equiv 1 \mod 2$.*
(e) *If u is even, then $(-1)^u = 1$.*
(f) *If u is odd, then $(-1)^u = -1$.*
(g) *We have $u = (u//2) \cdot 2 + (u\%2)$.*

Proof of Proposition 6.4. Parts **(a)**, **(b)**, **(c)** and **(d)** of Proposition 6.4 are parts of Exercise 3 on homework set #1, and their proofs can be found in the class notes. Thus, we only need to prove parts **(e)**, **(f)** and **(g)** now.

(e) Assume that that u is even. Then, $u \equiv 0 \bmod 2$ (by Proposition 6.4 **(c)**). In other words, $2 \mid u$. In other words, $u = 2g$ for some $g \in \mathbb{Z}$. Consider this g. From $u = 2g$, we obtain $(-1)^u = (-1)^{2g} = \Bigg(\underbrace{(-1)^2}_{=1}\Bigg)^g = 1^g = 1$. This proves Proposition 6.4 **(e)**.

(f) Assume that that u is odd. Then, $u \equiv 1 \bmod 2$ (by Proposition 6.4 **(d)**). In other words, $2 \mid u-1$. In other words, $u-1 = 2g$ for some $g \in \mathbb{Z}$. Consider this g. From $u-1 = 2g$, we obtain $(-1)^{u-1} = (-1)^{2g} = \Bigg(\underbrace{(-1)^2}_{=1}\Bigg)^g = 1^g = 1$. Now, $(-1)^u = (-1)\underbrace{(-1)^{u-1}}_{=1} = -1$. This proves Proposition 6.4 **(f)**.

(g) In Corollary 2.6.9 **(d)** of the class notes, we have proven $u = (u//n)\, n + (u\%n)$ for any positive integer n. Applying this to $n = 2$, we obtain $u = (u//2) \cdot 2 + (u\%2)$. This proves Proposition 6.4 **(g)**. □

In order to prove (5), we distinguish between two cases:

Case 1: The integer n is even.

Case 2: The integer n is odd.

Let us first consider Case 1. In this case, the integer n is even. Thus, $(-1)^n = 1$ (by Proposition 6.4 **(e)**, applied to $u = n$). Furthermore, n is even, and thus $n \equiv 0 \bmod 2$ (by Proposition 6.4 **(c)**, applied to $u = n$). Hence, $\underbrace{n}_{\equiv 0 \bmod 2} + 2 \equiv 0 + 2 = 2 \equiv 0 \bmod 2$. In other words, $n+2$ is even (by Proposition 6.4 **(c)**, applied to $u = n+2$). In other words,

$(n+2)\,\%2 = 0$ (by Proposition 6.4 **(a)**, applied to $u = n+2$). Now, Proposition 6.4 **(g)** (applied to $u = n+2$) yields

$$(n+2) = ((n+2)\,//2) \cdot 2 + \underbrace{((n+2)\,\%2)}_{=0} = ((n+2)\,//2) \cdot 2.$$

Solving this for $(n+2)\,//2$, we find $(n+2)\,//2 = (n+2)\,/2$.

Now,

$$\begin{aligned}
\sum_{k=0}^{n} (-1)^k (k+1) &= 1 - 2 + 3 - 4 \pm \cdots + \underbrace{(-1)^n}_{=1} (n+1) \\
&= 1 - 2 + 3 - 4 \pm \cdots + (n+1) \\
&= \underbrace{(1-2)}_{=-1} + \underbrace{(3-4)}_{=-1} + \underbrace{(5-6)}_{=-1} + \cdots + \underbrace{((n-1)-n)}_{=-1} + (n+1) \\
&= \underbrace{\underbrace{((-1)+(-1)+(-1)+\cdots+(-1))}_{n/2 \text{ addends}}}_{=n/2\cdot(-1)=-n/2} + (n+1) \\
&= -n/2 + (n+1) = n/2 + 1.
\end{aligned}$$

Comparing this with

$$\underbrace{(-1)^n}_{=1} ((n+2)\,//2) = (n+2)\,//2 = (n+2)\,/2 = n/2 + 1,$$

we obtain $\sum\limits_{k=0}^{n} (-1)^k (k+1) = (n+2)\,//2$. Hence, (5) is proved in Case 1.

Let us next consider Case 2. In this case, the integer n is odd. Thus, $(-1)^n = -1$ (by Proposition 6.4 **(f)**, applied to $u = n$). Furthermore, n is odd, and thus $n \equiv 1 \bmod 2$ (by Proposition 6.4 **(d)**, applied to $u = n$). Hence, $\underbrace{n}_{\equiv 1 \bmod 2} + 2 \equiv 1 + 2 = 3 \equiv 1 \bmod 2$. In other words, $n+2$ is odd (by Proposition 6.4 **(d)**, applied to $u = n+2$). In other words, $(n+2)\,\%2 = 1$ (by Proposition 6.4 **(b)**, applied to $u = n+2$). Now, Proposition 6.4 **(g)** (applied to $u = n+2$) yields

$$(n+2) = ((n+2)\,//2) \cdot 2 + \underbrace{((n+2)\,\%2)}_{=1} = ((n+2)\,//2) \cdot 2 + 1.$$

Solving this for $(n+2)\,//2$, we find $(n+2)\,//2 = ((n+2)-1)\,/2 = (n+1)\,/2$.

Now,

$$\begin{aligned}
\sum_{k=0}^{n} (-1)^k (k+1) &= 1 - 2 + 3 - 4 \pm \cdots + \underbrace{(-1)^n}_{=-1} (n+1) \\
&= 1 - 2 + 3 - 4 \pm \cdots - (n+1) \\
&= \underbrace{(1-2)}_{=-1} + \underbrace{(3-4)}_{=-1} + \underbrace{(5-6)}_{=-1} + \cdots + \underbrace{(n-(n+1))}_{=-1} \\
&= \underbrace{((-1)+(-1)+(-1)+\cdots+(-1))}_{(n+1)/2 \text{ addends}} \\
&= (n+1)\,/2 \cdot (-1) = -(n+1)\,/2.
\end{aligned}$$

Comparing this with

$$\underbrace{(-1)^n}_{=-1} \underbrace{((n+2)//2)}_{=(n+1)/2} = (-1)(n+1)/2 = -(n+1)/2,$$

we obtain $\sum\limits_{k=0}^{n} (-1)^k (k+1) = (n+2)//2$. Hence, (5) is proved in Case 2.

We have now proven (5) in each of the two Cases 1 and 2. Thus, (5) always holds. As explained above, by proving (5), we have solved the exercise.

6.3 Remark

I have posed this exercise in a slightly different form as Exercise 1 on homework set #9 of UMN Fall 2017 Math 4990. (The form was different in that I wrote $\left\lfloor \dfrac{n+2}{2} \right\rfloor$ instead of $(n+2)//2$. Of course, this is the same thing.) See also Angela Chen's solution to that exercise.

The exercise is more or less a combination of [Grinbe19, Exercise 2.9] and [Grinbe19, Exercise 3.5 **(b)**]. In fact, Lemma 6.3 above is the claim of [Grinbe19, Exercise 3.5 **(b)**], whereas the identity (5) is the claim of [Grinbe19, Exercise 2.9] (except that [Grinbe19, Exercise 2.9] writes $\begin{cases} n/2+1, & \text{if } n \text{ is even;} \\ (n+1)/2, & \text{if } n \text{ is odd} \end{cases}$ for $(n+2)//2$, but the equality of these two expressions is easy to establish).

Yet another way to state the identity in the exercise is

$$\sum_{k=0}^{n} \binom{-2}{k} = \frac{1+(-1)^n \cdot (2n+3)}{4}.$$

(Here, the "oscillator" $(-1)^n$ is being used instead of $(n+2)//2$ in order to obtain different behavior for even and odd n.) Similar identities are

$$\sum_{k=0}^{n} \binom{0}{k} = 1;$$
$$\sum_{k=0}^{n} \binom{-1}{k} = \frac{1+(-1)^n}{2} = (n+1)\,\%2;$$
$$\sum_{k=0}^{n} \binom{-3}{k} = \frac{1+(-1)^n \cdot (2n^2+8n+7)}{8};$$
$$\sum_{k=0}^{n} \binom{-4}{k} = \frac{3+(-1)^n \cdot (4n^3+30n^2+68n+45)}{48}.$$

More generally, I suspect that if $u \in \mathbb{N}$, then there is a polynomial $q_u(x)$ of degree u with rational coefficients such that each $n \in \mathbb{N}$ satisfies

$$\sum_{k=0}^{n} \binom{-(u+1)}{k} = \frac{1}{2^{u+1}} + (-1)^n \cdot q_u(n).$$

References

[GrKnPa94] Ronald L. Graham, Donald E. Knuth, Oren Patashnik, *Concrete Mathematics, Second Edition*, Addison-Wesley 1994.
See `https://www-cs-faculty.stanford.edu/~knuth/gkp.html` for errata.

[Grinbe19] Darij Grinberg, *Notes on the combinatorial fundamentals of algebra*, 10 January 2019.
`http://www.cip.ifi.lmu.de/~grinberg/primes2015/sols.pdf`
The numbering of theorems and formulas in this link might shift when the project gets updated; for a "frozen" version whose numbering is guaranteed to match that in the citations above, see `https://github.com/darijgr/detnotes/releases/tag/2019-01-10` .