

Math 4281: Introduction to Modern Algebra, Spring 2019: Midterm 1

Darij Grinberg

May 15, 2019

due date: **Wednesday, 6 March 2019** at the beginning of class,
or before that through Canvas.

No collaboration allowed – this is a midterm.
Please solve **at most 3 of the 6 exercises!**

1 EXERCISE 1: GCDS AND LCMS TOGETHER

1.1 PROBLEM

Let a, b, c be three integers.

(a) Prove that $\gcd(a, \operatorname{lcm}(b, c)) = \operatorname{lcm}(\gcd(a, b), \gcd(a, c))$.

(b) Prove that $\operatorname{lcm}(a, \gcd(b, c)) = \gcd(\operatorname{lcm}(a, b), \operatorname{lcm}(a, c))$.

1.2 SOLUTION

See the class notes, where this is Exercise 2.13.11.

2 EXERCISE 2: p -ADIC VALUATIONS OF RATIONALS

2.1 PROBLEM

Fix a prime p . For each nonzero rational number r , define the *extended p -adic valuation* $w_p(r)$ as follows: We write r in the form $r = a/b$ for two nonzero integers a and b , and set $w_p(r) = v_p(a) - v_p(b)$. (It also makes sense to set $w_p(0) = \infty$, but we shall not concern ourselves with this border case in this exercise.)

- (a) Prove that this is well-defined – i.e., that $w_p(r)$ does not depend on the precise choice of a and b satisfying $r = a/b$.
- (b) Prove that $w_p(n) = v_p(n)$ for each nonzero integer n .
- (c) Prove that $w_p(ab) = w_p(a) + w_p(b)$ for any two nonzero rational numbers a and b .
- (d) Prove that $w_p(a + b) \geq \min\{w_p(a), w_p(b)\}$ for any two nonzero rational numbers a and b if $a + b \neq 0$.

2.2 REMARK

The claim of part (d) has a curious (and, if you are a number theorist, important) consequence: Each prime p can be used to define a “distance function” on \mathbb{Q} that is very different from the usual distance function $((a, b) \mapsto |a - b|)$: Namely, for any two rational numbers a and b , we define the *p -adic distance* $d_p(a, b)$ between a and b by

$$d_p(a, b) = \begin{cases} p^{w_p(a-b)}, & \text{if } a - b \neq 0; \\ 0, & \text{if } a - b = 0. \end{cases}$$

For instance, $d_3(5, 1/2) = 3^{w_3(5-1/2)} = 3^2$, since $w_3(5 - 1/2) = w_3(9/2) = v_3(9) - v_3(2) = 2 - 0 = 2$.

The p -adic distance deserves the name “distance”, as it does satisfy the triangle inequality:

$$d_p(a, c) \leq d_p(a, b) + d_p(b, c) \quad \text{for any } a, b, c \in \mathbb{Q}.$$

Actually, the following stronger inequality (called *ultrametric triangle inequality*) holds:

$$d_p(a, c) \leq \max\{d_p(a, b), d_p(b, c)\} \quad \text{for any } a, b, c \in \mathbb{Q}.$$

Indeed, this follows easily from part (d) of the exercise (applied to $a - b$ and $b - c$ instead of a and b).

You might remember that the real numbers were defined as the completion of the rational numbers with respect to the usual distance (i.e., a real number is actually an equivalence class of Cauchy sequences defined with respect to the usual distance). Similarly one can consider the completion of the rational numbers with respect to the p -adic distance (i.e., again consider Cauchy sequences, but this time the distances are replaced by the p -adic distances). This leads to the p -adic numbers. See [Gouvea97] for an elementary introduction to this subject.

2.3 SOLUTION

See the class notes, where this is Exercise 3.4.1.

3 EXERCISE 3: HOW OFTEN DOES A PRIME DIVIDE A FACTORIAL?

3.1 PROBLEM

In this exercise, we shall use the *Iverson bracket notation*: If \mathcal{A} is any statement, then $[\mathcal{A}]$ stands for the integer $\begin{cases} 1, & \text{if } \mathcal{A} \text{ is true;} \\ 0, & \text{if } \mathcal{A} \text{ is false} \end{cases}$ (which is also known as the *truth value* of \mathcal{A}). For instance, $[1 + 1 = 2] = 1$ and $[1 + 1 = 1] = 0$.

- (a) Prove that $n//k = \sum_{i=1}^n [k \mid i]$ for any $n \in \mathbb{N}$ and any positive integer k .
- (b) Prove that $v_p(n) = \sum_{i \geq 1} [p^i \mid n]$ for any prime p and any nonzero integer n . Here, the sum $\sum_{i \geq 1} [p^i \mid n]$ is a sum over all positive integers; but it is well-defined, since it has only finitely many nonzero addends.
- (c) Prove that $v_p(n!) = \sum_{i \geq 1} n//p^i$ for any prime p and any $n \in \mathbb{N}$.

3.2 SOLUTION

See the class notes, where this is the first three parts of Exercise 2.17.2.

4 EXERCISE 4: WILSON WITH A TWIST

4.1 PROBLEM

Let p be a prime. Prove that

$$(p-1)! \equiv p-1 \pmod{1+2+\cdots+(p-1)}.$$

4.2 SOLUTION

See the class notes, where this is Exercise 2.15.4.

5 EXERCISE 5: GCDS IN EXPONENTS

5.1 PROBLEM

Let a be an integer. Let $n, m \in \mathbb{N}$. Prove that

$$\gcd(a^n - 1, a^m - 1) = |a^{\gcd(n, m)} - 1|.$$

[Hint: Strong induction. First show that $a^n - 1 \equiv a^m - 1 \pmod{a^{n-m} - 1}$ if $n \geq m$.]

5.2 SOLUTION

See the class notes, where this is Exercise 2.9.3 (with slightly changed notations).

6 EXERCISE 6: REMAINDER ARITHMETIC

6.1 PROBLEM

Let u and v be two integers. Let n be a positive integer. Prove that

$$u \% n + v \% n - (u + v) \% n \in \{0, n\}.$$

6.2 SOLUTION

See the class notes, where this is Exercise 2.6.3 (a).

REFERENCES

[Gouvea97] Fernando Q. Gouvea, *p-adic numbers: An introduction*, 2nd edition, Springer 1997. <https://www.springer.com/us/book/9783540629115> or <https://link.springer.com/book/10.1007/F978-3-642-59058-0>.