University of Minnesota, School of Mathematics

# 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

[...]

# 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:

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

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

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

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

[...]

# 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

[...]

---

# 4 Exercise 4: Wilson with a twist

## 4.1 Problem

Let $p$ be a prime. Prove that

$$(p-1)! \equiv p-1 \mod 1+2+\cdots+(p-1).$$

## 4.2 Solution

[...]

---

# 5 Exercise 5: gcds in exponents

## 5.1 Problem

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

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

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

### 5.2 Solution

[...]

---

## 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

[...]

## 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` .

[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` .