University of Minnesota, School of Mathematics

Math 4281: Introduction to Modern Algebra, Spring 2019: Homework 3

Darij Grinberg

May 15, 2019

due date: **Wednesday, 20 February 2019** at the beginning of class, or before that by email or canvas.
Please solve **at most 3 of the 6 exercises**!

1 Exercise 1: The Chinese remainder theorem for k moduli

1.1 Problem

Let $m_1, m_2, \ldots, m_k$ be k mutually coprime integers. Let $a_1, a_2, \ldots, a_k \in \mathbb{Z}$.
Prove the following:

(a) There exists an integer x such that

$$(x \equiv a_i \mod m_i \qquad \text{for all } i \in \{1, 2, \ldots, k\}).$$

(b) If x_1 and x_2 are two such integers x, then $x_1 \equiv x_2 \mod m_1 m_2 \cdots m_k$.

[**Note:** This is stated without proof in the lecture notes; you cannot just cite that statement.]

1.2 Solution

[...]

---

2 Exercise 2: More products of gcds

2.1 Problem

Let a, b, c be three integers.

(a) Prove that $\gcd(a, b) \gcd(a, c) = \gcd(ag, bc)$, where $g = \gcd(a, b, c)$.

(b) Assume that $b \perp c$. Prove that $\gcd(a, b) \gcd(a, c) = \gcd(a, bc)$.

2.2 Solution

[...]

---

3 Exercise 3: gcds and roots

3.1 Problem

Prove the following:

(a) If two integers a and b are not both zero, and if $g = \gcd(a, b)$, then $a/g \perp b/g$.

(b) If a and b are two integers, then $\gcd\left(a^k, b^k\right) = \gcd(a, b)^k$ for each $k \in \mathbb{N}$.

(c) If $r \in \mathbb{Q}$, then there exist two **coprime** integers a and b satisfying $r = a/b$.

(d) If a positive integer u is not a perfect square[1], then $\sqrt{u}$ is irrational.

(e) If u and v are two positive integers, then $\sqrt{u} + \sqrt{v}$ is irrational, unless both u and v are perfect squares.

3.2 Solution

[...]

---

[1] A *perfect square* means a square of an integer.

4 Exercise 4: Basic binomial congruences

4.1 Problem

Let p be a prime. Let $k \in \{0, 1, \ldots, p-1\}$. Prove the following:

(a) We have $k! \perp p$.

(b) If u and v are two integers such that $u \equiv v \mod p$, then $\dbinom{u}{k} \equiv \dbinom{v}{k} \mod p$.

(c) We have $\dbinom{p-1}{k} \equiv (-1)^k \mod p$.

4.2 Solution

[...]

---

5 Exercise 5: $\phi(n)$ is even

5.1 Problem

Let $n \in \mathbb{N}$ satisfy $n > 2$. Recall that ϕ denotes the Euler totient function. Prove that $\phi(n)$ is even.

[**Hint:** Is there a way to pair up the numbers $i \in \{1, 2, \ldots, n\}$ coprime to n?]

5.2 Solution

[...]

---

6 Exercise 6: $\phi\left(p^k\right)$

6.1 Problem

Let p be a prime. Let k be a positive integer. Prove that $\phi\left(p^k\right) = (p-1)\, p^{k-1}$.

6.2 Solution

[...]

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` .