Discrete Mathematics

Supervision 2

Marcelo Fiore   Ohad Kammar   Dima Szamozvancev

2. On numbers

2.1. Basic exercises

1. Let i, j be integers and let m, n be positive integers. Show that:
   a) $i \equiv i \pmod{m}$
   b) $i \equiv j \pmod{m} \implies j \equiv i \pmod{m}$
   c) $i \equiv j \pmod{m} \land j \equiv k \pmod{m} \implies i \equiv k \pmod{m}$
2. Prove that for all integers i, j, k, l, m, n with m positive and n nonnegative,
   a) $i \equiv j \pmod{m} \land k \equiv l \pmod{m} \implies i + k \equiv j + l \pmod{m}$
   b) $i \equiv j \pmod{m} \land k \equiv l \pmod{m} \implies i \cdot k \equiv j \cdot l \pmod{m}$
   c) $i \equiv j \pmod{m} \implies i^n \equiv j^n \pmod{m}$
3. Prove that for all natural numbers k, l and positive integers m,
   a) $\mathrm{rem}(k \cdot m + l, m) = \mathrm{rem}(l, m)$
   b) $\mathrm{rem}(k + l, m) = \mathrm{rem}(\mathrm{rem}(k, m) + l, m)$
   c) $\mathrm{rem}(k \cdot l, m) = \mathrm{rem}(k \cdot \mathrm{rem}(l, m), m)$
4. Let m be a positive integer.
   a) Prove the associativity of the addition and multiplication operations in $\mathbb{Z}_m$; that is:

   $$\forall i, j, k \in \mathbb{Z}_m.\ (i +_m j) +_m k = i +_m (j +_m k) \quad \text{and} \quad (i \cdot_m j) \cdot_m k = i \cdot_m (j \cdot_m k)$$

   b) Prove that the additive inverse of k in $\mathbb{Z}_m$ is $[-k]_m$.

2.2. Core exercises

1. Find an integer i, natural numbers k, l and a positive integer m for which $k \equiv l \pmod{m}$ holds while $i^k \equiv i^l \pmod{m}$ does not.
2. Formalise and prove the following statement: A natural number is a multiple of 3 iff so is the number obtained by summing its digits. Do the same for the analogous criterion for multiples of 9 and a similar condition for multiples of 11.
3. Show that for every integer n, the remainder when n^2 is divided by 4 is either 0 or 1.
4. What are $\mathrm{rem}(55^2, 79)$, $\mathrm{rem}(23^2, 79)$, $\mathrm{rem}(23 \cdot 55, 79)$ and $\mathrm{rem}(55^{78}, 79)$?
5. Calculate that $2^{153} \equiv 53 \pmod{153}$. At first sight this seems to contradict Fermat's Little Theorem, why isn't this the case though? *Hint:* Simplify the problem by applying known congruences to subexpressions using the properties in §2.1.2.

6. Calculate the addition and multiplication tables, and the additive and multiplicative inverses tables for $\mathbb{Z}_3$, $\mathbb{Z}_6$ and $\mathbb{Z}_7$.
7. Let i and n be positive integers and let p be a prime. Show that if $n \equiv 1 \pmod{p-1}$ then $i^n \equiv i \pmod{p}$ for all i not multiple of p.
8. Prove that $n^3 \equiv n \pmod{6}$ for all integers n.
9. Prove that $n^7 \equiv n \pmod{42}$ for all integers n.

2.3. Optional exercises

1. Prove that for all integers n, there exist natural numbers i and j such that $n = i^2 - j^2$ iff either $n \equiv 0 \pmod{4}$ or $n \equiv 1 \pmod{4}$ or $n \equiv 3 \pmod{4}$.
2. A *decimal* (respectively *binary*) *repunit* is a natural number whose decimal (respectively binary) representation consists solely of 1's.
   a) What are the first three decimal repunits? And the first three binary ones?
   b) Show that no decimal repunit strictly greater than 1 is a square, and that the same holds for binary repunits. Is this the case for every base? *Hint*: Use Lemma 26 of the notes.