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

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

(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 \(\gcd(a^k, b^k) = \gcd(a, b)^k\) 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 $\binom{u}{k} \equiv \binom{v}{k} \mod p$.

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

4.2 Solution

[...]

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

5.1 Problem
Let $n \in \mathbb{N}$ satisfy $n > 2$. Recall that $\phi$ 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: $\phi(p^k)$

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

6.2 Solution

[...]
REFERENCES

See [https://www-cs-faculty.stanford.edu/~knuth/gkp.html](https://www-cs-faculty.stanford.edu/~knuth/gkp.html) for errata.

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](https://github.com/darijgr/detnotes/releases/tag/2019-01-10).