Introduction to Number Theory (M328K)

Homework # 4

Fall 2025

Prof. Hector E. Lomeli

1. §3.3 # 32.

---

2. Let $a, x, y \in \mathbb{N}$.

a) Use the PMI to prove that the following predicate is true, for all $k \in \mathbb{N}$.

$$P(k) \Longleftrightarrow a^y - 1 \mid \left(a^y\right)^k - 1.$$

b) Prove that, if $y \mid x$, then $a^y - 1 \mid a^x - 1$.

3. Let $a, m, n \in \mathbb{N}$ with $a > 1$. We define $d_0 = a^{(m,n)} - 1$ and $d_1 = (a^m - 1, a^n - 1)$. Prove the following.

a) $d_0 | d_1$.

b) There exists $p, q \in \mathbb{N}$ such that

$$(m, n) = m\, p - n\, q.$$

c) If we let $u = a^{mp} - 1$ and $v = a^{nq} - 1$, then d_0 can be written as a linear combination of u and v.

d) $d_1 | d_0$ and therefore $d_0 = d_1$.

Use the Euclidean algorithm to find each of the following greatest common divisors. In each case, write the greatest common divisor of the integers as a linear combination of these integers. Justify your answer and show all your work.

4. (190, 25).

5. (800, 255)

6. (2000, 1001)