Solutions 04

P4.1. Let k, m, and n be integers satisfying $k > 1$ and $m > n \geqslant 0$. Use the Euclidean algorithm to prove that $\gcd(k^m - 1, k^n - 1) = k^{\gcd(m,n)} - 1$.

Solution. When $n = 0$, we have

$$\gcd(k^m - 1, k^0 - 1) = \gcd(k^m - 1, 1 - 1) = \gcd(k^m - 1, 0) = k^m - 1$$

and $k^{\gcd(m,0)} - 1 = k^m - 1$, so we may assume that $n > 0$. Since m and n are positive integers, the division algorithm implies that there exists nonnegative integers q and r such that $m = qn + r$ and $0 \leqslant r < n$. It follows that

$$\begin{aligned}\left(\sum_{i=1}^{q} k^{m-i\,n}\right)(k^n - 1) + (k^r - 1) &= \left(\sum_{i=1}^{q} k^{m-i\,n+n}\right) - \left(\sum_{i=1}^{q} k^{m-i\,n}\right) + (k^{m-qn} - 1)\\ &= k^m + \left(\sum_{i=2}^{q} k^{m-(i-1)n}\right) - \left(\sum_{i=1}^{q-1} k^{m-i\,n}\right) - k^{m-qn} + k^{m-qn} - 1\\ &= k^m + \left(\sum_{i=1}^{q-1} k^{m-in}\right) - \left(\sum_{i=1}^{q-1} k^{m-i\,n}\right) - 1\\ &= k^m - 1\,.\end{aligned}$$

Since $k > 1$ and $n > r$, it follows that $k^n > k^{n-1} > \cdots > k^r > \cdots > k^2 > k > 1$ and $k^n - 1 > k^r - 1$. From the uniqueness property of the division algorithm, we deduce that $(k^m - 1) \,\%\, (k^n - 1) = k^r - 1$ and

$$(k^m - 1) \,//\, (k^n - 1) = \sum_{i=1}^{q} k^{m-i\,n} = k^{m-n} + k^{m-2n} + \cdots + k^{m-qn}\,.$$

To calculate $\gcd(k^m - 1, k^n - 1)$ using the Euclidean algorithm, the recursive step replaces $\gcd(k^m - 1, k^n - 1)$ with $\gcd(k^n - 1, k^r - 1)$. Similarly, to calculate $\gcd(m, n)$ using the Euclidean algorithm, the recursive step replaces $\gcd(m, n)$ with $\gcd(n, r)$. Furthermore, the halting condition $k^r - 1 = 0$ in the first case is equivalent to the halting condition $r = 0$ in the second. Given the bijective correspondence between the Euclidean algorithm applied to $\gcd(k^m - 1, k^n - 1)$ and $\gcd(m, n)$, we conclude that $\gcd(k^m - 1, k^n - 1) = k^{\gcd(m,n)} - 1$. □

P4.2. **i.** Let m be an integer. Confirm that $m^2 \equiv 0 \mod 3$ or $m^2 \equiv 1 \mod 3$.
ii. Let p be a prime integer such that $p \geqslant 5$. Prove that $p^2 + 2$ is reducible.

Solution.

i. The subset $\{0, 1, 2\} \subset \mathbb{Z}$ is a system of distinct representatives for the congruence relation modulo 3. Since

$$0^2 = 0 \equiv 0 \mod 3 \qquad 1^2 = 1 \equiv 1 \mod 3 \qquad 2^2 = 4 \equiv 1 \mod 3\,,$$

we see that square of any integer is either congruent to 0 or 1 modulo 3. Moreover, the square of an integer is congruent to 0 modulo 3 if and only if the integer itself is congruent to 0 modulo 3.

ii. Being an irreducible integer, the only divisors of p are ± 1 and $\pm p$. As $p \geqslant 5$, it follows that p is not divisible by 3. Part **i** implies that $p^2 \equiv 1 \mod 3$, so we see that $p^2 + 2 \equiv 0 \mod 3$ and 3 divides $p^2 + 2$. Since $p^2 + 2 > 3$, we deduce that $p^2 + 2$ is reducible. □

P4.3. **i.** Consider the integer

$$m := \sum_{j=0}^{k} d_j \, 10^j$$

where k is a nonnegative integer and, for each j, the integer d_j satisfies $0 \leqslant d_j \leqslant 9$. Show that 11 divides m if and only if 11 divides $\sum_{j=0}^{k} (-1)^j \, d_j$.

ii. Using part **i**, determine if 11 divides 91 827 263.

Solution.

i. Since $10 \equiv -1 \mod 11$, it follows that

$$m = \sum_{j=0}^{k} d_j \, 10^j \equiv \sum_{j=0}^{k} d_j \, (-1)^j \equiv \sum_{j=0}^{k} (-1)^j \, d_j \mod 11 \, .$$

Therefore, we have $m \equiv 0 \mod 11$ if and only if $\sum_{j=0}^{k} (-1)^j \, d_j \equiv 0 \mod 11$.

ii. We have

$$91\,827\,263 \equiv 9 - 1 + 8 - 2 + 7 - 2 + 6 - 3 \equiv 22 \equiv -2 + 2 \equiv 0 \mod 11$$

so 11 divides 91 827 263. □