Homework 8

Arjun Koshal

March 11, 2022 (Revised April 26, 2022)

Problem 1

Theorem. *For any two positive integers n and d, there are unique integers q and r such that $n = qd + r$ and $0 \leq r < d$.*

Proof. To prove this, we must first establish the existence of these integers, q, r, and then show that they are unique.

First we notice that if $n = d$, then $q = 1$ and we have $r = 0$ as the unique solution to the equation.

To establish the existence of such integers, we define for each $m \geq 0$, we have $r_m = n - md$. Let $S = \{r_m \mid r_m \geq 0\}$, that is, S is the set of r_m which is non-negative, and we know that r_0 must be greater than 0 as $r_0 = n$, which implies S is nonempty. Since the set S is well-ordered, as it is a subset of $\mathbb{N} \cup \{0\}$, we can state that S has a minimum element. We can denote this minimum element as $r_k = n - kd$ and it follows that $n = kd + r_k$. By looking at $k + 1$, it must hold that $r_{k+1} = n-(k+1)d = n-kd-d$. Then it follows that $r_{k+1} = r_k - d$, since $r_k = n-kd$. Since r_k is the minimum of S, r_{k+1} is not an element of S. However, $r_{k+1} < 0$, so it holds that $r_{k+1} = r_k - d < 0$ and thus $r_k < d$. Therefore there exists integers r_k and k such that $n = kd + r_k$ and $0 \leq r_k < d$. WLOG, we can state that there must exist integers q, r such that $n = qd + r$.

To show that these integers q and r are unique, suppose we have $n = q_1 d + r_1$ and $n = q_2 d + r_2$, where $q_1, q_2, r_1, r_2 \in \mathbb{Z}$, and $0 \leq r_1, r_2 < d$. Then it must hold that,

$$\begin{aligned} q_1 d + r_1 &= q_2 d + r_2 \\ q_1 d - q_2 d &= r_2 - r_1 \\ d(q_1 - q_2) &= r_2 - r_1. \end{aligned}$$

Thus, $d|(r_2 - r_2)$. Since $0 \leq r_1 < d$ and $0 \leq r_2 < d$, it must hold that $-d < r_2 - r_1 < d$. We know that $d|(r_2 - r_1)$ is true if and only if $r_2 - r_1 = 0$, therefore we can state $r_1 = r_2$. If $q_1 - q_2 > 0$, then $d(q_1 - q_2) \geq d$, which is not possible, and if $q_1 - q_2 \leq 0$, then $d(q_1 - q_2) < -d$, which is not possible as well. Therefore it must hold true that $d(q_1 - q_2) = 0$. Since $d > 0$, $q_1 - q_2 = 0$, which leads to $q_1 = q_2$. Thus, the integers q and r are unique. $\square$

Problem 2

Theorem. *Every natural number can be written in the form rs^2, where $r, s \in \mathbb{N}$ and r is square-free.*

Proof. If $n = 1$, then it follows that $r = s = 1$.

By the fundamental theorem of arithmetic, we can write n as a product of primes, that is, $n = p_1 p_2 ... p_k$ where $p_1, p_2, ... p_k$ are primes. Then we have the following 3 cases:

Case 1: If every prime in $p_1, p_2, ... p_k$ is distinct, since all primes are trivially square-free, n must be true such that $s = 1$ and $r = p_1, p_2, ... p_k$.
Case 2: If there exists a prime, p_t in $p_1, p_2, ... p_k$ that occurs an m number of times, where $m = 2u, u \in \mathbb{Z}$, then we can factor out $p_t^{(2u)}$. Then n must be true such that $s = p_t^{(u)}$ and $r = 1$.
Case 3: If there exists a prime, p_t in $p_1, p_2, ... p_k$ that occurs an m number of times, where $m = 2v + 1, v \in \mathbb{Z}$, then we can factor out $p_t^{(2v+1)}$. Then n must be true such that $s = p_t^{(m)}$ and $r = p_t$.

Now let us group the terms that meet either cases 2 or 3 in $p_1, p_2, ... p_k$, and it follows that the remaining terms must follow case 1. Let r be the product of r's determined in all cases and let s be the product of s's in all cases. Thus, it must hold every natural number n must have the decomposition $n = rs^2$, where r is square-free. ☐

Problem 3

Theorem. *Every prime greater than 3 is one away from a multiple of $3! = 6$.*

Proof. Let us represent any natural number n as the sum $n = 6d + r$, $0 \leq r < 6$, where d is an integer. Through this representation, for n to be one away from a multiple of 6, we have $r = 1, 5$. Let us consider the cases for other possible r:

Case 1: $r = 0$: We have $n = 6d$ which is divisible by 6 and thus composite.
Case 2: $r = 2$: We have $n = 6d + 2$ which is even and thus composite, unless $n = 2$.
Case 3: $r = 3$: We have $n = 6d + 3 = 3(2d + 1)$ which is divisible by 3 and thus composite, unless $n = 3$.
Case 4: $r = 4$: We have $n = 6d + 4 = 2(3d + 2)$ which is even and thus composite.

Since these cases encompass equivalence classes of numbers mod 6 spanning all natural numbers, it follows that since prime numbers (greater than 3) do not exist in these equivalence classes, they must exist in either of the other two; by example, we know that $n = 7$ is in the equivalence class [1] and $n = 5$ is in the equivalence class [5], so primes exist in both classes. It follows that every prime greater than 3 must be one away from a multiple of 3!. ☐