Math 110AH Fall 18

HOMEWORK 2 - SOLUTIONS

Problem 1. Given two positive integers k, l, we will denote by $k^{(l)}$ the product of the l consecutive integers $k, k-1, \dots k-l+1$. We start by dealing with consecutive *positive* integers. Denote by $P(n)$ the property "$n!$ divides the product of any n consecutive positive integers".

- Since $1! = 1$ divides any integer, $P(1)$ is true.
- Assume $P(n)$ is true. To prove $P(n+1)$, we prove by induction on $m \geqslant n+1$ the property $Q(m)$: "$(n+1)!$ divides $m^{(n+1)}$".
  - We have $(n+1)^{(n+1)} = (n+1)!$, which is indeed a multiple of $(n+1)!$. So $Q(n+1)$ is true.
  - Assume that $Q(m)$ is true. Then we have:

$$\begin{aligned}(m+1)^{(n+1)} - m^{(n+1)} &= m^{(n)}\,(m+1-(m-n)) \\ &= m^{(n)}\,(n+1)\end{aligned}$$

    By $P(n)$, $n!$ divides $m^{(n)}$. So $(n+1)!$ divides $m^{(n)}\,(n+1)$. Furthermore, by $Q(m)$, $(n+1)!$ divides $m^{(n+1)}$. Thus $(n+1)!$ divides $m^{(n)}\,(n+1) + m^{(n+1)}$, which is equal to $(m+1)^{(n+1)}$ by the equation above. Hence $Q(m+1)$ is proved.

  So by the induction principle, $Q(m)$ is true for all $m \geqslant n+1$. This proves $P(n+1)$ and ends the proof of the main induction.

To finish the proof, we need to treat the case of negative integers. If $0 \leqslant m < n$ then $m^{(n)} = 0$. If $m < 0$, then $m^{(n)} = (-1)^n(-m+n-1)^{(n)}$, which is divisible by $n!$ by $P(n)$.

In conclusion, for any integers $n \geqslant 1$ and m, $n!$ divides $m^{(n)}$.

4.17 - Problem 2. The division algorithm for polynomials is stated in this way:

Theorem 1. *Let $A, B \in F[t]$ with $B \neq 0$. There exists unique $Q, R \in F[t]$ such that $A = BQ + R$, and $R = 0$ or $\deg(R) < \deg(B)$.*

Let us start by proving existence. Fix $B \neq 0$, and let $d = \deg(B)$. We can express B in the canonical basis:

$$B = \sum_{i=0}^{d} b_i t^i$$

for some $b_i \in F$, $b_d \neq 0$. We prove the result by strong induction on $\deg(A)$.

- If $A = 0$ or $\deg(A) < d$, we have $A = B \cdot 0 + A$ in the desired form.
- Assume we have proved the result for all polynomials of degree at most k, for some $k \geqslant d-1$. Let A be a polynomial of degree $k+1$. Let us express A in the canonical basis:

$$A = \sum_{i=0}^{k+1} a_i t^i$$

for some $a_i \in F$, $a_{k+1} \neq 0$. Consider the polynomial:

$$A' := A - \frac{a_{k+1}}{b_d} t^{k+1-d} B$$

By looking at the coefficients of A' we see that either $A' = 0$ or $\deg(A') \leqslant k$. Thus by induction we can find Q, R such that $A' = BQ + R$ and $R = 0$ or $\deg(R) < d$. So $A = B(Q + \frac{a_{k+1}}{b_d} t^{k+1-d}) + R$ with $R = 0$ or $\deg(R) < d$, and we are done.

Let us now prove uniqueness. Given A, B, assume that we have (Q, R) and (Q', R') satisfying the theorem. Then $BQ + R = BQ' + R'$. This can be written $R - R' = B(Q' - Q)$. So $R - R'$ is a multiple of B. However, all non-zero multiples of B have degree at least $\deg(B)$, and $R - R'$ is either 0 or of degree less than $\deg(B)$. Hence $R - R' = 0$, which proves the uniqueness of R.
Our equation above now gives $B(Q' - Q) = 0$. The product of two non-zero polynomials is non-zero, and $B \neq 0$. Hence $Q' - Q = 0$, which proves the uniqueness of Q. In conclusion (Q, R) is unique.

4.17 - Problem 4. We construct the sequences $(q_i)_{i \geqslant 1}$, $(r_i)_{i \geqslant 0}$ by induction.

- Define $r_0 = b$, and q_1 and r_1 as the quotient and the remainder of the Euclidean division of a by b. Then we have $0 \leqslant r_1 < b$.
- Assume we have constructed $q_1, \ldots, q_i$ and $r_0, \ldots, r_i$ for some $i \geqslant 1$. If $r_i \neq 0$, define q_{i+1} and r_{i+1} to be the quotient and the remainder of the Euclidean division of r_{i-1} by r_i. Then we have $0 \leqslant r_{i+1} < r_i$. If $r_i = 0$, we let $q_{i+1} = r_{i+1} = 0$.

Necessarily, $r_i = 0$ for i large enough. Indeed, the construction shows that otherwise (r_i) would be a decreasing sequence of natural integers, which does not exist. Hence, we can define $k = \min\{i;\, r_{i+1} = 0\}$. The theorem is proved.

4.17 - Problem 6. We use the Euclidean algorithm to find a particular solution:

$$\begin{aligned} 39493 &= 19853 + 19640 \\ 19853 &= 19640 + 213 \\ 19640 &= 213 \cdot 92 + 44 \\ 213 &= 44 \cdot 4 + 37 \\ 44 &= 37 + 7 \\ 37 &= 7 \cdot 5 + 2 \\ 7 &= 2 \cdot 3 + 1 \\ 2 &= 2 \cdot 1 + 0 \end{aligned}$$

Painstakingly, we find the particular solution $X_0 = 8575$, $Y_0 = -17058$. The solutions of the equation are thus $(X_0 + k19853, Y_0 - k39493)$ for $k \in \mathbb{Z}$.

4.17 - Problem 8. For the statement of this problem to be true, we have to assume that $p > 1$.

Assume that p be a prime. It is a well-known result from class that for all $a, b \in \mathbb{Z}$, if $p|ab$ then $p|a$ or $p|b$.

Conversely, assume that for all $a, b \in \mathbb{Z}$, if $p|ab$ then $p|a$ or $p|b$. Let us prove that p is prime. Let d be a divisor of p, we have $p = du$ for some $u \in \mathbb{Z}$. Then $p|du$, so by assumption $p|d$ or $p|u$. If $p|d$, p and d divide each other so $d = \pm p$. If $p|u$, p and u divide each other so $u = \pm p$, and $d = \pm 1$. Hence the only divisors of p are ± 1 and $\pm p$, so p is prime.

Problem 3. Let n be any integer. Then we have $n + 1 - n = 1$. By property 4.9 (1) from the textbook, we deduce that $(n, n + 1) = 1$.

Problem 4. By a theorem seen in class, we know that the smallest positive integer in $\{120a + 28b;\ a, b \in \mathbb{Z}\}$ is the gcd of 120 and 28. We can compute that gcd by the Euclidean algorithm:

$$\begin{aligned} 128 &= 28 \cdot 4 + 16 \\ 28 &= 16 \cdot 1 + 12 \\ 16 &= 12 \cdot 1 + 4 \\ 12 &= 4 \cdot 3 + 0 \end{aligned}$$

The gdc is thus 4.

So we can find $s, t \in \mathbb{Z}$ such that $4 = 128s + 28t$. Multiplying by 2 gives us $8 = 128(2s) + 28(2t)$, so 8 can be expressed as a linear combination of 128 and 28 (the numbers

that can be expressed like this are precisely the multiples of the gcd, as seen in class).

To find the coefficients explicitly, it suffices to run through the Euclidean algorithm written above. We find that $4 = 2 \cdot 128 - 9 \cdot 28$. Thus $8 = 4 \cdot 128 - 18 \cdot 28$.

Problem 5. The result false if $n = 0$, so consider an integer $n > 0$. Let a, b be two integers. Assume first that $a|b$. Then by definition $b = au$ for some $u \in \mathbb{Z}$. Thus we get $a^n = b^n u^n$. So $a^n|b^n$.

Conversely, assume that $a^n|b^n$. Let us write the prime decompositions of a and b:

$$a = \prod_{i=1}^{r} p_i^{\alpha_i}$$

$$b = \prod_{i=1}^{r} p_i^{\beta_i}$$

where $(p_i)_{1 \leqslant i \leqslant r}$ are distinct primes and $\alpha_i, \beta_i \in \mathbb{N}$. Consider $1 \leqslant j \leqslant r$, the assumption $a^n|b^n$ tells us in particular that $p_j^{n\alpha_j} | \prod_{i=1}^{r} p_i^{n\beta_i}$. But if $i \neq j$, $p_j^{n\alpha_j}$ and $p_i^{n\beta_i}$ are relatively prime. So we get that $p_j^{n\alpha_j} | p_j^{n\beta_j}$. Hence $n\alpha_j \leqslant n\beta_j$. Since $n > 0$, this gives $\alpha_j \leqslant \beta_j$. So we get the following factorization:

$$b = a \prod_{i=1}^{r} p_i^{\beta_i - \alpha_i}$$

and it follows that $a|b$.

Problem 6. (a) Not reflexive, not symmetric, not transitive.

(b) Not reflexive, symmetric, not transitive.

(c) Not reflexive, not symmetric, not transitive.

(d) Not reflexive, symmetric, not transitive.

(e) This is an equivalence relation. The easiest way to see this is to remark that:

$$5|(x + 4y) \;\Leftrightarrow\; 5|(x - y).$$

This is because $5|5y$. So if $5|(x + 4y)$, we have $5|(x + 4y - 5y) = (x - y)$. Conversely, if $5|x - y$, we have $5|(x - y + 5y) = (x + 4y)$. So R is the usual equivalence relation modulo 5, and its equivalence classes are the equivalence classes modulo 5.

Problem 7. Let $(a,b) \in \mathbb{N} \times \mathbb{N}$. Then we have $a+b = b+a$, so $(a,b) \sim (a,b)$: the relation $\sim$ is reflexive. Assume $(a,b) \sim (c,d)$, then $a+d = b+c$, so $c+b = d+a$, and $(c,d) \sim (a,b)$: the relation $\sim$ is symmetric. Assume $(a,b) \sim (c,d)$ and $(c,d) \sim (e,f)$, then we have $a+d = b+c$ and $c+f = d+e$. We deduce from this that:

$$a+f = a+d+e-c = b+c+e-c = b+e$$

So $(a,b) \sim (e,f)$: the relation $\sim$ is transitive. In conclusion, the relation $\sim$ is an equivalence relation.

Let $(a,b) \in \mathbb{N} \times \mathbb{N}$, and let $k = a-b$. Then the equivalence class of (a,b) consists of all the points of $(c,d) \in \mathbb{N} \times \mathbb{N}$ such that $d = c-k$: it is a "line" of "slope" 1 and "y-intercept" $-k$. So the set of equivalence classes is the set of "lines of slope 1" in $\mathbb{N} \times \mathbb{N}$.