391 Homework 3 solutions

- Exercises 1.1: 4(e), 18.

4(e) For \( n \geq 3, n + 4 < 2^n \).

   **Proof.** Proceed by induction on \( n = 3, 4, \ldots \).

   **Base case.** If \( n = 3, 3 + 4 = 7 < 8 = 2^3 \).

   **Induction step:** Assume true for \( n = k, i.e. k + 4 < 2^k \). Consider the inequality for \( n = k + 1 \). We have that \( k + 5 = k + 4 + 1 < 2^k + 1 < 2^k + 2^k = 2^{k+1} \). Done.

18. Prove by induction that for any \( k = 1, 2, \ldots \), the product of \( k \) consecutive integers is divisible by \( k! \).

   **Proof. I am going to show by induction on \( m = n + k \) that \((n + 1) \ldots (n + k)\) is divisible by \( k! \) for every \( n = 0, 1, \ldots \) and \( k = 1, 2, \ldots \).**

   **Base case:** If \( m = 1, i.e. n = 0, k = 1, this is obvious.**

   **Induction step:** Assume that \((n + 1) \ldots (n + k)\) is divisible by \( k! \) for every \( n, k \) with \( n + k < r \). Suppose instead that we are given \( n, k \) with \( n + k = r \), and consider \((n + 1)(n + 2) \ldots (n + k)\). If \( k = 1 \) or if \( n = 1 \), the conclusion is obvious, so we may assume in addition that \( k > 1 \) and \( n > 1 \).

   By the induction hypothesis (and the assumption \( k > 1 \) and \( n > 1 \)), \( n(n+1) \ldots (n+k-1) \) is divisible by \( k! \) and \((n+1) \ldots (n+k-1)\) is divisible by \((k-1)!\). Now write

   \[(n+1) \ldots (n+k) = n(n+1) \ldots (n+k-1) + k(n+1) \ldots (n+k-1)\].

   The first term on the RHS is divisible by \( k! \), while the second term on the RHS is \( k \) times something divisible by \((k-1)!\), hence is also divisible by \( k! \). Hence the LHS is divisible by \( k! \) too. This completes the induction step.

   We have now established that \((n+1) \ldots (n+k)\) is divisible by \( k! \) for every \( n = 0, 1, \ldots \) and \( k = 1, 2, \ldots \). Strictly speaking we are not quite done, because the question asked for \( k \) consecutive integers, possibly negative! But in general, given \( k \) consecutive integers \((n+1) \ldots (n+k)\) with \( n \) negative, we can choose \( x \) so that \( n + xk! \) is positive. Then by what we have shown already,

   \[(n + xk! + 1) \ldots (n + xk! + k)\]
is divisible by $k!$. Expanding the brackets, it equals

$$(n + 1) \ldots (n + k) + (\text{a multiple of } k!).$$

So we get too that $(n+1) \ldots (n+k)$ is divisible by $k!$ in the general case.

- Exercises 1.2: 9, 10, 11, 17.

9. Prove that if $p$ is prime and $p|(a_1 \ldots a_n)$ then $p|a_j$ for some $j$.

Proceed by induction on $n$. If $n = 1$ there is nothing to prove, so the base case is okay. For the induction step, assume that $p|(a_1 \ldots a_{n-1})$ implies that $p|a_j$ for some $j$, for every product $a_1 \ldots a_{n-1}$ of $(n-1)$ integers. Now consider the product of $n$ (maybe different!) integers, $b_1 \ldots b_n$.

If $p|b_1 \ldots b_n$, then $p|xb_n$ where $x = b_1 \ldots b_{n-1}$. By Proposition 2.5, since $p$ is prime, we get that either $p|x$ or $p|b_n$. In the latter case, we are done already. In the former case, $p|b_1 \ldots b_{n-1}$, whence by the induction hypothesis, $p|b_j$ for some $j$. This completes the proof.

10. Given a positive integer $n$, find $n$ consecutive composite numbers.

The numbers are

$$(n + 1)! + 2, (n + 1)! + 3, \ldots, (n + 1)! + n.(n + 1)! + (n + 1).$$

Obviously the first is divisible by 2, so composite, the second by 3, so composite,..., the nth by $(n + 1)$ so composite.

11. Prove that there are no integers $m, n$ so that $\left(\frac{m}{n}\right)^2 = 2$.

Suppose for a contradiction that there are integers $m, n$ so that $\left(\frac{m}{n}\right)^2 = 2$. We may assume that $m, n$ are relatively prime (since otherwise we could simplify the fraction). Then,

$$m^2 = 2n^2.$$ 

Hence, $m^2$ is even, which implies that $m$ is even, i.e. $m = 2k$ for some integer $k$. But then

$$m^2 = 4k^2 = 2n^2$$
2k^2 = n^2.

This means that \( n^2 \) is even, which implies that \( n \) is even too. Now we have shown that both \( m \) and \( n \) are divisible by 2, which contradicts our original assumption that \( m \) and \( n \) were relatively prime.

17. Prove that whenever \( n > 1 \) is odd, \( 2^{mn} + 1 \) is a composite number.

Proof. Let \( r = -2^m \). Then, assuming that \( n > 1 \) is odd,

\[
1 + r + \ldots + r^{n-1} = \frac{r^n - 1}{r - 1} = \frac{(-2^m)^n - 1}{-2^m - 1} = \frac{2^{mn} + 1}{2^m + 1}
\]

using Example 2 from 1.1 and the fact that \( n \) is odd. Hence,

\[
2^{mn} + 1 = (2^m + 1)(1 + r + \ldots + r^{n-1})
\]

is a composite number since \( 2^m + 1 \) is a factor.

• Exercises 1.3: 1, 2(b), 4, 5.

1. We need to check three things. First: \( a \equiv a \pmod{m} \).

Proof. By definition this means that \( m | (a - a) \), which is true as everything divides 0.

Second: \( a \equiv b \pmod{m} \) implies \( b \equiv a \pmod{m} \).

Proof. If \( a \equiv b \pmod{m} \), then \( m | (b - a) \), hence \( m | (a - b) \), hence \( b \equiv a \pmod{m} \).

Third: If \( a \equiv b \pmod{m} \) and \( b \equiv c \pmod{m} \) then \( a \equiv c \pmod{m} \).

Proof. We have that \( m | (b - a) \) and \( m | (c - b) \). Hence, \( m | (b - a) + (c - b) = (c - a) \), i.e. \( a \equiv c \pmod{m} \).

2(b) Say \( n = \sum_{i=0}^{k} a_i 10^i \). Show that \( 3 | n \) if and only if \( 3 | \sum_{i=0}^{k} a_i \).

Proof. Note that \( 10 \equiv 1 \pmod{3} \), hence \( 10^i \equiv 1 \pmod{3} \) for each \( i \geq 0 \). So,

\[
n \equiv \sum_{i=0}^{k} a_i 10^i \equiv \sum_{i=0}^{k} a_i \pmod{3}.
\]

Now \( 3 | n \) if and only if \( n \equiv 0 \pmod{3} \), so we have shown that \( 3 | n \) if and only if \( 3 | \sum_{i=0}^{k} a_i \) as we wanted.
4. They switch sides after 1, 3, 5, 7, ... games. This means that after 0 games, he is on side A, after 1 or 2 games he is on side B, after 3 or 4 games he is on side A again, .... In other words if you look at the total number of games played modulo 4 and you get 0 or 3, he is on the side he started on, if you get 1 or 2 he is on the other side.

Now, \( \bar{6} + \bar{2} + \bar{4} + \bar{3} = \bar{3} \) and \( \bar{6} + \bar{2} + \bar{5} + \bar{4} = \bar{1} \). Hence since is is on the side he started on, the score must be \( 6 - 2, 4 - 3 \).

5. Prove that for any integer \( n \), \( n^2 \equiv 0 \text{ or } 1 \pmod{3} \), and \( n^2 \equiv 0, 1 \text{ or } 4 \pmod{5} \).

To calculate the possibilities for \( n^2 \mod 3 \), we only need to consider \( n = 0, 1, 2 \). Now \( \bar{0}^2 = \bar{0}, \bar{1}^2 = \bar{1} \) and \( \bar{2}^2 = \bar{1} \). So the squares modulo 3 are \( \bar{0} \) and \( \bar{1} \) only.

Instead modulo 5, \( \bar{0}^2 = \bar{0}, \bar{1}^2 = \bar{1}, \bar{2}^2 = \bar{4}, \bar{3}^2 = \bar{9} = \bar{4} \) and \( \bar{4}^2 = \bar{1} \).

So the squares modulo 5 are \( \bar{0}, \bar{1} \) and \( \bar{4} \) only.