HW2 Solutions

1.72 Let $n = p^r m$, where p is a prime not dividing an integer $m \geq 1$. Prove that $p \nmid \binom{n}{p^r}$.

Solution. Write $a = \binom{n}{p^r}$. By Pascal's formula:

$$a = \binom{n}{p^r} = \frac{n!}{(p^r)!(n - p^r)!}.$$

Cancel the factor $(n - p^r)!$ and cross-multiply, obtaining:

$$a(p^r)! = n(n-1)(n-2)\cdots(n - p^r + 1).$$

Thus, the factors on the right side, other than $n = p^r m$, have the form $n - i = p^r m - i$, where $1 \leq i \leq p^r - 1$. Similarly, the factors in $(p^r)!$, other than p^r itself, have the form $p^r - i$, for i in the same range: $1 \leq i \leq p^r - 1$.

If $p^e \mid p^r m - i$, where $e \leq r$ and $i \geq 1$, then $p^r m - i = bp^e$; hence, $p^e \mid i$; there is a factorization $i = p^e j$. Therefore, $p^r - i = p^e(p^{r-e} - j)$.

A similar argument shows that if $p^e \mid p^r - i$ for $i \geq 1$, then $p^e \mid p^r m - i$. By the fundamental theorem of arithmetic, the total number of factors p occurring on each side must be the same. Therefore, the total number of p's dividing ap^r must equal the total number of p's dividing $p^r m$. Since $p \nmid m$, the highest power of p dividing $p^r m$ is p^r, and so the highest power of p dividing ap^r is p^r; that is, $p \nmid a = \binom{p^r m}{p^r} = \binom{n}{p^r}$, as desired.

1.73 **(i)** For all rationals a and b, prove that

$$\|ab\|_p = \|a\|_p \|b\|_p \quad \text{and} \quad \|a+b\|_p \leq \max\{\|a\|_p, \|b\|_p\}.$$

Solution. If $a = p^e p_1^{e_1} \cdots p_n^{e_n}$ and $b = p^f p_1^{f_1} \cdots p_n^{f_n}$, then

$$ab = p^{e+f} p_1^{e_1+f_1} \cdots p_n^{e_n+f_n}.$$

Hence

$$\|ab\|_p = p^{-e-f} = p^{-e} p^{-f} = \|a\|_p \|b\|_p.$$

Assume $e \leq f$, so that $-f \leq -e$ and $\|a\|_p = \max\{\|a\|_p, \|b\|_p\}$.

$$\begin{aligned} a+b &= p^e p_1^{e_1} \cdots p_n^{e_n} + p^f p_1^{f_1} \cdots p_n^{f_n} \\ &= p^e \left(p_1^{e_1} \cdots p_n^{e_n} + p^{f-e} p_1^{f_1} \cdots p_n^{f_n} \right). \end{aligned}$$

If $u = p_1^{e_1} \cdots p_n^{e_n} + p^{f-e} p_1^{f_1} \cdots p_n^{f_n}$, then either $u = 0$ or $\|u\|_p = p^{-0} = 1$. In the first case, $\|a+b\|_p = 0$, and the result is true. Otherwise,

$$\begin{aligned} \|a+b\|_p = p^{-e}\|u\|_p &= \|a\|_p \|u\|_p \\ &\leq \|a\|_p = \max\{\|a\|_p, \|b\|_p\}. \end{aligned}$$

(ii) For all rationals a, b, prove $\delta_p(a,b) \geq 0$ and $\delta_p(a,b) = 0$ if and only if $a = b$.

Solution. $\delta_p(a,b) \geq 0$ because $\|c\|p \geq 0$ for all c. If $a = b$, then $\delta_p(a,b) = \|a-b\|p = \|0\|p = 0$; conversely, if $\delta_p(a,b) = 0$, then $a - b = 0$ because 0 is the only element c with $\|c\|_p = 0$.

(iii) For all rationals a, b, prove that $\delta_p(a,b) = \delta_p(b,a)$.

Solution. $\delta_p(a,b) = \delta_p(b,a)$ because

$$\|-c\|p = \|-1\|p\|c\|_p = \|c\|_p.$$

(iv) For all rationals a, b, c, prove $\delta_p(a, b) \le \delta_p(a, c) + \delta_p(c, b)$.
Solution. $\delta_p(a, b) \le \delta_p(a, c) + \delta_p(c, b)$ because

$$\begin{aligned}\delta_p(a, b) &= \|a - b\|_p = \|(a - c) + (c - b)\|_p \\ &\le \max\{\|a - c\|_p, \|c - b\|_p\} \\ &\|a - c\|_p + \|c - b\|_p \\ &= \delta_p(a, c) + \delta_p(c, b).\end{aligned}$$

(v) If a and b are integers and $p^n \mid (a - b)$, then $\delta_p(a, b) \le p^{-n}$. (Thus, a and b are "close" if $a - b$ is divisible by a "large" power of p.)
Solution. If $p^n \mid a - b$, then $a - b = p^n u$, where u is an integer. But $\|u\|_p \le 1$ for every integer u, so that

$$\delta_(a, b) = \|a - b\|_p = \|p^n u\|_p = \|p^n\|_p \|u\|_p \le p^{-n}.$$

At this point, one could assign a project involving completions, p-adic integers, and p-adic numbers.

1.81 What is the remainder after dividing 10^{100} by 7?
Solution. Use Corollary 1.67 after noting that $100 = 2 \cdot 7^2 + 2$ (of course, this says that 100 has 7-adic digits 202). Hence

$$10^{100} \equiv 3^{100} \equiv 3^4 = 81 \equiv 4 \bmod 7.$$

1.83 **(i)** Show that $1000 \equiv -1 \bmod 7$.
Solution. Dividing 1000 by 7 leaves remainder $6 \equiv -1 \bmod 7$.

(ii) Show that if $a = r_0 + 1000 r_1 + 1000^2 r_2 + \cdots$, then a is divisible by 7 if and only if $r_0 - r_1 + r_2 - \cdots$ is divisible by 7.
Solution. If $a = r_0 + 1000 r_1 + 1000^2 r_2 + \cdots$, then

$$a \equiv r_0 + (-1) r_1 + (-1)^2 r_2 + \cdots = r_0 - r_1 + r_2 - \cdots \bmod 7.$$

Hence a is divisible by 7 if and only if $r_0 - r_1 + r_2 - \cdots$ is divisible by 7.

1.87 If x is an odd number not divisible by 3, prove that $x^2 \equiv 1 \bmod 24$.
Solution. Here are two ways to proceed. The odd numbers < 24 not divisible by 3 are 1, 5, 7, 11, 13, 17, 19, 23; square each mod 24.

Alternatively, Example 1.161 says that the squares mod 8 are 0, 1, and 4. Now $x^2 - 1$ is divisible by 24 if and only if it is divisible by 3 and by 8 (as 3 and 8 are relatively prime). If x is to be odd, then $x \equiv 0 \bmod 3$ or $x \equiv 2 \bmod 3$; looking at $x \bmod 8$, the hypothesis eliminates those x with $x^2 \equiv 0 \bmod 8$ or $x^2 \equiv 4 \bmod 8$.