

3 About Homework 3:

1.51. If a, b are relatively prime and $a|n, b|n$ then $ab|n$.

Ans: There are integers x, y so that

$$ax + by = 1.$$

Since a, b divide n we have $n = as$ and $n = bt$ for some s, t . So

$$n = axn + byn = axbt + byas = ab(xt + ys)$$

proving that n is a multiple of ab .

1.55. (i) $\gcd(a, b, c) = \gcd(a, \gcd(b, c))$

Ans: Let $e = \gcd(b, c)$ and $d = \gcd(a, e) = \gcd(a, \gcd(b, c))$. Then, d divides a and $e = \gcd(b, c)$. But b, c are both multiples of e so d divides b, c as well. Therefore, d divides a, b, c , i.e., it is a common divisor of a, b, c and as such cannot be greater than the greatest common divisor:

$$d \leq \gcd(a, b, c).$$

On the other hand, by problem 1.54, we know that $\gcd(a, b, c)$ is the smallest possible positive integer which is a linear combination of a, b, c . Since d is also a linear combination of a, b, c (since $e = bx + cy$ and $d = as + et = as + bxt + cyt$) we must have

$$d \geq \gcd(a, b, c).$$

Therefore, $d = \gcd(a, b, c)$.

1.63. If $n = p^r m$ where p, m are relatively prime then p does not divide $\binom{n}{p^r}$.

Ans1: Using the method taught in class: the number of times that p divides the binomial coefficient

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

is given by

$$\sum_{k \geq 1} \left[\frac{n}{p^k} \right] - \sum_{k \geq 1} \left[\frac{p^r}{p^k} \right] - \sum_{k \geq 1} \left[\frac{n - p^r}{p^k} \right]. \quad (1)$$

We need to calculate this and show that it is zero. The second sum is the easiest to calculate:

$$\sum_{k \geq 1} \left[\frac{p^r}{p^k} \right] = \sum_{k=1}^r p^{r-k} = 1 + p + p^2 + \cdots + p^{r-1} = \frac{1 - p^r}{1 - p}$$

The first and third sum are similar. Since $n = p^r m$ we get:

$$\sum_{k \geq 1} \left[\frac{n}{p^k} \right] = \sum_{k=1}^r p^{r-k} m + \sum_{k > r} \left[\frac{m}{p^{k-r}} \right] = \left(\frac{1-p^r}{1-p} \right) m + \sum_{j \geq 1} \left[\frac{m}{p^j} \right]$$

Since $n - p^r = p^r(m - 1)$ we have:

$$\sum_{k \geq 1} \left[\frac{n - p^r}{p^k} \right] = \sum_{k=1}^r p^{r-k}(m-1) + \sum_{k > r} \left[\frac{m-1}{p^{k-r}} \right] = \left(\frac{1-p^r}{1-p} \right) (m-1) + \sum_{j \geq 1} \left[\frac{m-1}{p^j} \right]$$

Plug these into the expression (1) and we get

$$\left(\frac{1-p^r}{1-p} \right) m - \frac{1-p^r}{1-p} - \left(\frac{1-p^r}{1-p} \right) (m-1) = 0$$

plus

$$\sum_{j \geq 1} \left[\frac{m}{p^j} \right] - \sum_{j \geq 1} \left[\frac{m-1}{p^j} \right]$$

This is also zero since

$$\sum_{j \geq 1} \left[\frac{m}{p^j} \right]$$

is the number of times that p divides $m!$ which is equal to

$$\sum_{j \geq 1} \left[\frac{m-1}{p^j} \right]$$

which is the number of times that p divides $(m-1)!$.

Ans2. There are easier proofs. One is the following.

$$\binom{n}{p^r} = \frac{n(n-1)(n-2)(n-3) \cdots (n-p^r+1)}{1 \cdot 2 \cdot 3 \cdots (p^r-1) \cdot p} = \frac{n}{p^r} \prod_{k=1}^{p^r-1} \frac{n-k}{k}$$

But $\frac{n}{p^r} = m$ and, in each of the fractions $\frac{n-k}{k}$, I claim that p divides the top and bottom the same number of times. To prove this write $k = p^a x$ where $(p, x) = 1$. Then $a < r$ since $k < p^r$. Therefore,

$$n - k = p^r - p^a x = p^a (p^{r-a} - x)$$

where $p^{r-a} - x \equiv -x \pmod{p}$ is relatively prime to p . Thus p divides the numerator and denominator of $\binom{n}{p^r}$ the same number of times.

Ans3. The binomial coefficient $\binom{n}{p^r}$ is defined to be the coefficient of x^{p^r} in $(1+x)^n$. Since $n = p^r m$ we have

$$\begin{aligned} (1+x)^n &= ((1+x)^{p^r})^m \equiv (1+x^{p^r})^m \pmod{p} \\ &= 1 + mx^{p^r} + \binom{m}{2} x^{2p^r} + \cdots \end{aligned}$$

so $\binom{n}{p^r} \equiv m \pmod{p}$ is not divisible by p .