

What's  $\nu_p$ ?

Math 453  
8/31/07  
Bonus Notes

Suppose  $p$  is prime and  $n \geq 1$  is an integer.

We define  $\nu_p(n)$  to be the exponent of  $p$  in the prime factorization of  $n$ ;  $\nu_p(n) = 0$  if  $p$  does not divide  $n$ . If  $p^a | n$  and  $p^{a+1} \nmid n$  (or  $p^a || n$  - see HW 72, p. 34), then  $\nu_p(n) = a$ .

Ex:  $n = 2^3 \cdot 3^2 = 72$ , so  $\nu_2(72) = 3$ ,  $\nu_3(72) = 2$ ,  $\nu_5(72) = 0$ ,  $\nu_7(72) = 0$  etc..

$$\text{For every } n \geq 1, \quad n = 2^{\nu_2(n)} \cdot 3^{\nu_3(n)} \cdot 5^{\nu_5(n)} \cdot 7^{\nu_7(n)} \cdots$$
$$= \prod_{p \text{ prime}} p^{\nu_p(n)}$$

①  $\nu_p(m \cdot n) = \nu_p(m) + \nu_p(n)$ , so  $\nu_p$  is a "discrete log"

The proof of this fact is that if we let  $\{p_1, \dots, p_r\}$  denote the primes in either the factorization of  $m$  or of  $n$ , and allow  $a_i, b_i \geq 0$ , then

$$m = \prod_{i=1}^r p_i^{a_i}, \quad n = \prod_{i=1}^r p_i^{b_i} \Rightarrow m \cdot n = \prod_{i=1}^r p_i^{a_i + b_i}$$

②  $a | b \iff \nu_p(a) \leq \nu_p(b)$  for all primes  $p$ .

$\Rightarrow a | b \Rightarrow b = a \cdot c$ , so  $\nu_p(b) = \nu_p(a) + \nu_p(c)$ .

Since  $\nu_p(c) \geq 0$  for all integers  $c$ ,  $\nu_p(b) \geq \nu_p(a)$ .

$\Leftarrow$  Let  $\Gamma_p = \nu_p(b) - \nu_p(a) \geq 0$  for all primes  $p$ .

Let  $c = \prod_{p \text{ prime}} p^{\Gamma_p}$ . Then  $\nu_p(c) = \nu_p(b) - \nu_p(a)$

so  $c \cdot a = b$  and  $a | b$



Intuitive proof: Each multiple of  $p \leq n$  contributes one factor of  $p$  to  $n!$ . Each multiple of  $p^2 \leq n$  contributes a second factor of  $p$ , etc. There are  $\lfloor \frac{n}{p} \rfloor$  multiples of  $p \leq n$ ,  $\lfloor \frac{n}{p^2} \rfloor$  multiples of  $p^2 \leq n$ , etc. ...

$$\begin{aligned} \text{ex } \lfloor \frac{10}{2} \rfloor + \lfloor \frac{10}{4} \rfloor + \lfloor \frac{10}{8} \rfloor + \lfloor \frac{10}{16} \rfloor + \dots &= 5 + 2 + 1 + 0 + \dots = 8 \\ \lfloor \frac{10}{3} \rfloor + \lfloor \frac{10}{9} \rfloor + \lfloor \frac{10}{27} \rfloor + \dots &= 3 + 1 = 4 \quad \lfloor \frac{10}{5} \rfloor + \lfloor \frac{10}{25} \rfloor + \dots = 2 + 0 = 2 \\ \lfloor \frac{10}{7} \rfloor + \lfloor \frac{10}{49} \rfloor + \dots &= 1 + 0 + \dots = 1 \end{aligned}$$

Rigorous proof by induction.

$$\nu_p(1!) = \nu_p(1) = 0 = \sum_{k \geq 1} \lfloor \frac{1}{p^k} \rfloor, \text{ since } \frac{1}{p^k} < 1 \text{ for every prime } p \text{ and } k \geq 1.$$

Assume the formula holds for  $n-1$ .

$$\nu_p((n-1)!) = \sum_{k \geq 1} \lfloor \frac{n-1}{p^k} \rfloor$$

$$n! = (n-1)! \cdot n, \text{ so } \nu_p(n!) = \nu_p((n-1)!) + \nu_p(n).$$

$$\text{so } \nu_p(n!) = \sum_{k \geq 1} \lfloor \frac{n-1}{p^k} \rfloor + \nu_p(n).$$

We want this to equal  $\sum_{k \geq 1} \lfloor \frac{n}{p^k} \rfloor$ , so we calculate the difference.

$$\sum_{k \geq 1} \lfloor \frac{n}{p^k} \rfloor - \nu_p(n!) = \sum_{k \geq 1} \lfloor \frac{n}{p^k} \rfloor - \left( \sum_{k \geq 1} \lfloor \frac{n-1}{p^k} \rfloor + \nu_p(n) \right)$$

$$= \sum_{k \geq 1} \left( \lfloor \frac{n}{p^k} \rfloor - \lfloor \frac{n-1}{p^k} \rfloor \right) - \nu_p(n). \text{ By the observation,}$$

$$\lfloor \frac{n}{p^k} \rfloor - \lfloor \frac{n-1}{p^k} \rfloor = 1 \text{ only if } p^k | n.$$

If  $\nu_p(n) = a$ , then this is true for  $k = 1, \dots, a$ ,

$$\text{Thus, } \sum_{k \geq 1} \lfloor \frac{n}{p^k} \rfloor - \nu_p(n!) = \underbrace{1 + \dots + 1}_{\nu_p(n)} - \nu_p(n) = 0 \quad \square$$

Example 25!

$$v_2(25!) = \lfloor \frac{25}{2} \rfloor + \lfloor \frac{25}{4} \rfloor + \lfloor \frac{25}{8} \rfloor + \lfloor \frac{25}{16} \rfloor + \lfloor \frac{25}{32} \rfloor + \dots$$
$$= 12 + 6 + 3 + 1 = 22$$

$$v_3(25!) = \lfloor \frac{25}{3} \rfloor + \lfloor \frac{25}{9} \rfloor + \lfloor \frac{25}{27} \rfloor + \dots$$
$$= 8 + 2 = 10$$

$$v_5(25!) = \lfloor \frac{25}{5} \rfloor + \lfloor \frac{25}{25} \rfloor + \dots = 5 + 1 = 6$$

If  $7 < p < 25$ , Then  $\lfloor \frac{25}{p^2} \rfloor = \lfloor \frac{25}{p^3} \rfloor = \dots = 0$ .

$$v_7(25!) = \lfloor \frac{25}{7} \rfloor = 3, \quad v_{11}(25!) = \lfloor \frac{25}{11} \rfloor = 2, \quad v_{13}(25!) = \lfloor \frac{25}{13} \rfloor = 1,$$
$$v_{17}(25!) = \lfloor \frac{25}{17} \rfloor = 1, \quad v_{19}(25!) = \lfloor \frac{25}{19} \rfloor = 1, \quad v_{23}(25!) = \lfloor \frac{25}{23} \rfloor = 1$$

$$\text{So } 25! = 2^{22} 3^{10} 5^6 7^3 11^2 \cdot 13 \cdot 17 \cdot 19 \cdot 23$$

Mathematica tells me it's 155 112100433309859840000000

The binomial coefficient  $\binom{n}{m}$  for integers  $m, n$

with  $0 \leq m \leq n$  is defined to be

$$\frac{n!}{m!(n-m)!} \quad \text{It is always an integer.}$$

and  $m!(n-m)! \binom{n}{m} = n!$  implies that

$$v_p \left( \binom{n}{m} \right) = v_p(n!) - v_p(m!) - v_p(n-m!)$$

We can say more, but that's for another handout