UCD

Mathematics Enrichment Programme 2013

Two lectures on inequalities related to number theory.

Thomas J. Laffey

March 23 2013

April 6 2013

Square bracket function: x a real number.

$[x]$ denotes the <u>greatest</u> integer k not exceeding x. [1]

So $[11/3] = 3$ since $3 \leq \frac{11}{3} < 4$.

$[4] = 4$, $[4{\cdot}37] = 4$, $[-1{\cdot}6] = -2$.

If a, b are positive integers, we can write
$$a = bq + r$$
where $q \geq 0$ and r are <u>integers</u> with $0 \leq r < b$.

Then $\frac{a}{b} = q + \frac{r}{b}$ and $0 \leq \frac{r}{b} < 1$.

So $[\frac{a}{b}] = q$.

<u>Problem</u>. Let n be a positive integer and p a prime. We want to find a formula for the greatest integer k for which p^k divides $n!$.

<u>Solution</u>: List the numbers
$$1, 2, 3, \ldots, n$$
Pick out the multiples of p in the list
$$1p, 2p, 3p, \ldots, ap \qquad a = [\tfrac{n}{p}]$$
We get an obvious factor p^a from the product of these. We now look for extra powers of p from the product of
$$1, 2, 3, \ldots, a.$$

Pick out the multiples of p in this list.

$$1p,\ 2p,\ 3p,\ \cdots,\ bp \quad , \quad b = \left[\frac{a}{p}\right].$$

We then get the obvious factor p^b from the product. We then look for extra powers from the product of $1, 2, 3, \cdots, b$. Pick out the multiples of p: $1p,\ 2p,\ 3p,\ \cdots,\ cp$, $c = \left[\frac{b}{p}\right]$ and get the obvious factor p^c and then look at $1, 2, 3, \cdots, c$. Proceed until we have no multiples of p left.

Note that $b = \left[\frac{a}{p}\right]$ and $a = \left[\frac{n}{p}\right]$, so $b = \left[\frac{n}{p^2}\right]$ (why?). Also $c = \left[\frac{b}{p}\right]$ and $b = \left[\frac{n}{p^2}\right]$, so $c = \left[\frac{n}{p^3}\right]$ (why?),

and so on.

The total power of p dividing $n!$ is

$$p^a\, p^b\, p^c \cdots \quad = \quad p^k \quad \text{where}$$

$$\begin{aligned} k &= a + b + c + \cdots \\ &= \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \cdots \end{aligned}$$

Notice that this can be written

$$k = \sum_{\gamma=1}^{\infty} \left[\frac{n}{p^\gamma}\right].$$

[All the terms $\left[\frac{n}{p^\gamma}\right] = 0$ for $p^\gamma > n$, so this is really a finite sum].

Example 1. The highest power 2^k dividing $100!$ is given by
$$k = \left[\frac{100}{2}\right] + \left[\frac{100}{2^2}\right] + \left[\frac{100}{2^3}\right] + \left[\frac{100}{2^4}\right] + \left[\frac{100}{2^5}\right] + \left[\frac{100}{2^6}\right]$$
$$= 50 + 25 + 12 + 6 + 3 + 1$$
$$= 97.$$

The largest integer l for which 5^l divides $100!$ is
$$l = \left[\frac{100}{5}\right] + \left[\frac{100}{5^2}\right] = 20 + 4 = 24.$$

To calculate the number of zeros at the end when $100!$ is written out in ordinary decimal (= base 10) form, we need to know the highest power of 10 which divides $100!$. But to make a factor 10 we require a factor 2 and a factor 5. Now $100!$ has the factor 2 a ~~total~~ total of 97 times and the factor 5 a total of 24 times. So $100!$ has the factor 10 a ~~total~~ of 24 times. So $100!$ ends in 24 zeros.

More generally, $n!$ ends in k zeros where k is the highest exponent for which 10^k divides $n!$ and this is the same as the highest exponent k for which 5^k divides $n!$. So $k = \sum_{j=1}^{\infty} \left[\frac{n}{5^j}\right]$.

Example 2. Find a positive integer n for which $n!$ ends in 2013 zeros or prove that no such n exists. [4]

Solution. The highest exponent k for which 5^k divides $n!$ $\leq \frac{n}{5} + \frac{n}{5^2} + \frac{n}{5^3} + \cdots$

$= \frac{n}{5} \frac{1}{1-\frac{1}{5}}$ (using the formula for summing a geometric progression)

$= n/4$.

So we start with $4 \times 2013 = 8052$.

The highest exponent k_0 for which 5^{k_0} divides

$$8052! = \left[\frac{8052}{5}\right] + \left[\frac{8052}{5^2}\right] + \left[\frac{8052}{5^3}\right] + \left[\frac{8052}{5^4}\right] + \left[\frac{8052}{5^5}\right] \quad (\text{since } 5^6 > 8052)$$

$= 1610 + 322 + 64 + 12 + 2$

$= 2010$.

Hence $8055!$ is divisible by 5^{2011} and not 5^{2012}

$8060!$ .. 5^{2012} .... 5^{2013}

$8065!$ .... 5^{2013} and not by 5^{2014}.

Hence $8065!$ ends in 2013 zeros

A variation on the formula.

Write n in base p, that is write 5

$$n = a_0 + a_1 p + a_2 p^2 + \cdots + a_r p^r$$

where $a_0, a_1, \ldots, a_r$ are integers with $0 \le a_j \le p-1$ for all j and $a_r \ne 0$.

Then
$$\left[\frac{n}{p}\right] = a_1 + a_2 p + a_3 p^2 + \cdots + a_r p^{r-1}$$
$$\left[\frac{n}{p^2}\right] = a_2 + a_3 p + \cdots + a_r p^{r-2}$$
$$\left[\frac{n}{p^3}\right] = a_3 + \cdots + a_r p^{r-3}$$
$$\vdots$$
$$\left[\frac{n}{p^r}\right] = \cdots a_r .$$
$$\left[\frac{n}{p^j}\right] = 0 \text{ for } j > r.$$

So
$$\sum_{j=1}^{\infty}\left[\frac{n}{p^j}\right] = a_1 + a_2(1+p) + a_3(1+p+p^2) + \cdots + a_r(1+p+\cdots+p^{r-1})$$
$$= a_1 + a_2\left(\frac{p^2-1}{p-1}\right) + a_3\left(\frac{p^3-1}{p-1}\right) + \cdots + a_r\left(\frac{p^r-1}{p-1}\right)$$

and $a_1 = \dfrac{a_1(p-1)}{p-1}$.

So
$$\sum_{j=1}^{\infty}\left[\frac{n}{p^j}\right] = \frac{a_1 p + a_2 p^2 + \cdots + a_r p^r - (a_1 + a_2 + \cdots + a_r)}{p-1}$$
$$= \frac{a_0 + a_1 p + a_2 p^2 + \cdots + a_r p^r - (a_0 + a_1 + \cdots + a_r)}{p-1}$$
$$= \frac{n - (a_0 + a_1 + \cdots + a_r)}{p-1}.$$

So if p^k divides $n!$, then

$$k = \frac{n-(a_0+\dots+a_r)}{p-1} \leq \frac{n-1}{p-1},$$

so $k < n$.

So p^n does not divide $n!$

<u>Example 3</u> Let $n > 1$ be an integer and

$$f(x) = 1 + x + \frac{x^2}{2!} + \frac{x^2}{3!} + \dots + \frac{x^n}{n!}.$$

Prove that the equation $f(x) = 0$ has no integer solution.

<u>Solution.</u> Suppose for the sake of contradiction that $f(\alpha) = 0$ for some integer α.

Now $f(1) > 0$, so $\alpha \neq 1$. Also

$$f(-1) = 1 - 1 + \frac{1}{2!} - \frac{1}{3!} + \frac{1}{4!} - \dots + \frac{(-1)^n}{n!}$$

But $\frac{1}{3!} + \frac{1}{4!} + \dots + \frac{1}{n!} < \frac{1}{4} + \frac{1}{8} + \frac{1}{16} + \dots$

$$= \frac{1}{4}\,\frac{1}{1-1/2} = 1/2.$$

So $f(-1) > 0$.

So $\alpha \neq \pm 1$. So α is divisible by some prime p. Since p^m does not divide $m!$ for any positive integer m, in lowest form each of the fractions $\frac{\alpha^j}{j!}$

has its numerator (top) divisible by p. So when we form the sum

$$s = \alpha + \frac{\alpha^2}{2!} + \frac{\alpha^3}{3!} + \cdots + \frac{\alpha^n}{n!}$$

we get a fraction $\frac{pa}{b}$ where a, b are integers with p not dividing b.

So this sum s cannot be -1 and $f(\alpha) \neq 0$, contradicting our hypothesis.

So the result is proved.

The highest power of p dividing $\binom{2n}{n}$.

$\binom{2n}{n} = \frac{(2n)!}{(n!)^2}$. Write $2n$ in base p, say

$$2n = b_0 + b_1 p + b_2 p^2 + \cdots + b_t p^t,$$

where $0 \leq b_j \leq p-1$ and $b_t \neq 0$.

Then $\sum_{j=1}^{\infty}\left(\left[\frac{2n}{p^j}\right] - 2\left[\frac{n}{p^j}\right]\right) = \sum_{j=1}^{t}\left(\left[\frac{2n}{p^j}\right] - 2\left[\frac{n}{p^j}\right]\right)$

But note that $\left[\frac{2n}{p^j}\right] - 2\left[\frac{n}{p^j}\right] = 0$ or 1

For write $n = p^j q + r$ where q, r are integers with $0 \leq r < p^j$. Then $2n = p^j(2q) + 2r$ and $0 \leq 2r < 2p^j$. So $\left[\frac{n}{p^j}\right] = q$ and $\left[\frac{2n}{p^j}\right] = 2q$ or $2q+1$ depending on whether $2r < p^j$ or $2r \geq p^j$.

So $\sum_{j=1}^{\infty}\left(\left[\frac{2n}{p^j}\right] - 2\left[\frac{n}{p^j}\right]\right) \leq t$.

Let s be the greatest integer for which p^s divides $\binom{2n}{n}$. Then $s \le t$ and thus $p^s \le p^t \le 2n$. 8

An estimate for the number of prime numbers not exceeding $2n$.

Let $p_1 = 2, p_2 = 3, \ldots, p_r$ be the prime numbers $\le 2n$. Then $\binom{2n}{n} = p_1^{b_1} p_2^{b_2} \cdots p_r^{b_r}$ for some nonnegative integers $b_1, b_2, \ldots, b_r$ and, by the previous result, $p_j^{b_j} \le 2n$ for all j.

Hence $(2n)^r \geqslant \binom{2n}{n}$ . . . (X)

We now estimate the size of $\binom{2n}{n}$.

For $1 \le i < n$, $\binom{2n}{i} = \dfrac{2n(2n-1)\cdots(2n-i+1)}{i!}$

$$= \frac{2n(2n-1)\cdots(2n-i+1)(2n-i)}{i!\,(i+1)} \cdot \frac{i+1}{2n-i}$$

$$= \binom{2n}{i+1} \cdot \frac{i+1}{2n-i} < \binom{2n}{i+1}.$$

Also $\binom{2n}{2n-i} = \binom{2n}{i}$. Hence $\binom{2n}{n}$ is the largest of the numbers $1, \binom{2n}{1}, \binom{2n}{2}, \binom{2n}{3}, \ldots, \binom{2n}{2n}$

(Each binomial coefficient $\binom{2n}{i}$ is a integer greater than 1 for $1 \le i \le 2n-1$).

By the binomial theorem

$$2^{2n} = (1+1)^{2n} = 1 + \binom{2n}{1} + \binom{2n}{2} + \cdots + \binom{2n}{2n-1} + 1$$

So $$4^n = 2^{2n} = 2 + \binom{2n}{1} + \binom{2n}{2} + \cdots + \binom{2n}{n} + \cdots + \binom{2n}{2n-1}$$

There are $2n-1$ terms $\binom{2n}{1}, \binom{2n}{2}, \ldots, \binom{2n}{2n-1}$ and the biggest one is $\binom{2n}{n}$. Hence

$$4^n - 2 \le (2n-1)\binom{2n}{n}$$ and thus

$$\binom{2n}{n} \ge \frac{4^n - 2}{2n-1}.$$

Next
$$\frac{4^n-2}{2n-1} - \frac{4^n}{2n} = \frac{(2n)4^n - 4n - (2n)4^n + 4^n}{(2n-1)(2n)} = \frac{4^n - 4n}{(2n-1)(2n)}.$$

<u>Claim</u> $4^n > 4n$ for $n \geq 2$.
The result holds for $n = 2$, since $4^2 = 16 > 8 = 4 \times 2$. Proceeding by induction on n, suppose $k \geq 2$ is an integer and $4^k > 4k$. Then $4^{k+1} > 16k$ and $16k > 4(k+1)$, so the inequality holds for $k+1$. So by induction, the claim is proved.

Hence $$\frac{4^n-2}{2n-1} > \frac{4^n}{2n} \text{ for } n \geq 2$$ and

$$\binom{2n}{n} > \frac{4^n}{2n} \text{ for } n \geq 2.$$

But now, if r is the number of primes $\leq 2n$,

by (*), $$(2n)^r \geq \binom{2n}{n} > \frac{4^n}{2n} \text{ for } n \geq 2$$

and thus $$(r+1)\log(2n) > n\log 4$$ and
$$r+1 > \frac{n \log 4}{\log(2n)}, \text{ for } n \geq 2.$$

For example, taking $n = 50$, $r+1 > 15$ and $r > 14$, so, since r is an integer, $r \geq 15$. [The actual number is 25].

The function $\pi(x)$ = number of prime numbers not exceeding x. The last result states that

$$\pi(2n) + 1 > \frac{n \log 4}{\log(2n)} . \qquad \boxed{10}$$

Suppose p is a prime with $n < p \leq 2n$. Then p divides $(2n)!$ and p does not divide $(n!)^2$, so p divides $\binom{2n}{n}$.

Let h be the number of such primes. So $h = \pi(2n) - \pi(n)$ and, since each prime p in this range contributes a factor $\geq n+1$ $> n$ to $\binom{2n}{n}$, we get

$$n^h \leq \binom{2n}{n} < 4^n$$

so

$$h < \frac{n \log 4}{\log n} ,$$

that is

$$\pi(2n) - \pi(n) < \frac{n \log 4}{\log n} .$$

The arguments relating the number of primes to the binomial coefficient $\binom{2n}{n}$ is due to Tchebychef (Čebyšev). ($\sim$1850).
