PRIME FACTORS OF BINOMIAL COEFFICIENTS

SAMIN RIASAT

On a usual day, let's assume you are thinking about big numbers, say factorials, and digits, say 0 (must have been quite a bizzare day!). A common question that might pop up in your mind could be,

how many zeros are there at the end of 1000! ?

You may already know the answer. I certainly do, it's 249, because I read it in a book a long tme ago and for some weird reason it hasn't left my mind since then! You may also know how to find it. But just in case you don't, here's how to do it.

To find the number of zeros, we just need to find how many times the factors 2 and 5 appear in the prime factorization of 1000!. But there is already a large supply of factors of 2, so we need only find how many times the factor 5 appears. That's easy, there are $\lfloor 1000/5 \rfloor = 200$ factors of 5, each contributing at least a 5 in the prime factorization of 1000!. But hang on, there are also factors of $5^2 = 25$ each of which contributes an extra 5. There are $\lfloor 1000/5^2 \rfloor = 40$ such factors. Similarly, each factor of $5^3 = 125$ contributes even one more 5, and each factor of $5^4 = 625$ again contributes one more 5. We don't need to worry about 5^5 as there are no factors of 5^5 between 1 and 1000. Thus our answer is

$$\left\lfloor \frac{1000}{5} \right\rfloor + \left\lfloor \frac{1000}{5^2} \right\rfloor + \left\lfloor \frac{1000}{5^3} \right\rfloor + \left\lfloor \frac{1000}{5^4} \right\rfloor = 200 + 40 + 8 + 1 = 249.$$

Ha, my memory didn't fail me!

After coming this far, you are probably thinking about generalizing this. Indeed, it very easily generalizes to the following theorem attributed to Legendre [1]. Henceforth, n, r are positive integers with $r \le n$ and p is a prime. We will also say *the exponent of* p *in* x to mean the exponent of p in the prime factorization of x.

Theorem 1. *The exponent of* p *in* $n!$ *is given by*

$$\left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \cdots = \sum_{j=1}^{\infty} \left\lfloor \frac{n}{p^j} \right\rfloor .$$

Why do we sum up to infinity? More importantly, why should p be prime? I shall leave these to you to worry about.

So now we know how to find the exponent of p in $n!$. We can do more and find the exponent of p in $n!/r!$, or even better, $n!/r!(n-r)!$, the binomial coefficient $\binom{n}{r}$. Binomial coefficients are important numbers, so it should be worth investigating their prime factors.

Proposition 2. *The exponent of p in $\binom{n}{r}$ is* $\displaystyle\sum_{j=1}^{\infty}\left(\left\lfloor\frac{n}{p^j}\right\rfloor-\left\lfloor\frac{r}{p^j}\right\rfloor-\left\lfloor\frac{n-r}{p^j}\right\rfloor\right)$.

There is an advantage in writing the sum in the above form.

Proposition 3. *For real numbers a, b, $\lfloor a+b\rfloor-\lfloor a\rfloor-\lfloor b\rfloor\in\{0,1\}$.*

Proof. Writing $\{x\}$ for $x-\lfloor x\rfloor$ we need to show that

$$\{a\}+\{b\}-\{a+b\}\in\{0,1\}.$$

Note that $\{a+b\}=\{\{a\}+\{b\}\}$. So if $\{a\}+\{b\}<1$, $\{a+b\}=\{a\}+\{b\}$, otherwise $1\le\{a\}+\{b\}<2$ so $\{a+b\}+1=\{a\}+\{b\}$. □

Hence it follows that the value of each bracket in the sum in **Proposition 2** is equal to either 0 or 1. Therefore the exponent of p is precisely the number of brackets which equal 1. From the above proof,

$$\left\lfloor\frac{n}{p^j}\right\rfloor-\left\lfloor\frac{r}{p^j}\right\rfloor-\left\lfloor\frac{n-r}{p^j}\right\rfloor=1 \text{ if and only if } \left\{\frac{r}{p^j}\right\}+\left\{\frac{n-r}{p^j}\right\}\ge 1.$$

Although this is a good criterion to check whether a prime divides a binomial coefficient, it isn't used very much in practice. Nevertheless, we can deduce some quick facts from this. For example, if r and $n-r$ are both odd, then $\left\{\frac{r}{2}\right\}+\left\{\frac{n-r}{2}\right\}=\frac{1}{2}+\frac{1}{2}=1$. So we have proved that

Proposition 4. *If n is even and r is odd, then $\binom{n}{r}$ is even.*

In fact, we can do better.

Proposition 5. *If the exponent of 2 in n is greater than the exponent of 2 in r, then $\binom{n}{r}$ is even.*

Proof. Let $r=2^qa$, $n=2^qb$, with a odd and b even. Then $n-r=2^q(b-a)$, and since $b-a$ is odd,

$$\left\{\frac{r}{2^{q+1}}\right\}+\left\{\frac{n-r}{2^{q+1}}\right\}=\left\{\frac{a}{2}\right\}+\left\{\frac{b-a}{2}\right\}=\frac{1}{2}+\frac{1}{2}=1.$$

□

We can use our ideas to investigate the odd and even entries in Pascal's triangle. If we denote the odd and even entries by black dots and blanks, respectively, we will get a beautiful fractal called the Sierpinski triangle [2] (see figure 1).

But first let's go back to **Proposition 2** and see if we can find a better criterion. There are powers of p everywhere, which suggests us to look at things in base p. Let the base p representations of n, r and $n-r$ be

$$n=\overline{a_ka_{k-1}\dots a_1a_0}=a_kp^k+a_{k-1}p^{k-1}+\dots+a_1p+a_0$$
$$r=\overline{b_kb_{k-1}\dots b_1b_0}=b_kp^k+b_{k-1}p^{k-1}+\dots+b_1p+b_0$$
$$n-r=\overline{c_kc_{k-1}\dots c_1c_0}=c_kp^k+c_{k-1}p^{k-1}+\dots+c_1p+c_0$$

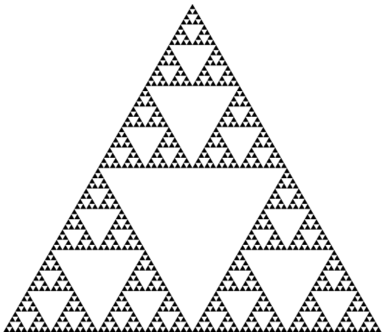

FIGURE 1. Sierpinski triangle

where $a_k \neq 0$. Then

$$\left\lfloor \frac{n}{p^j} \right\rfloor = a_k p^{k-j} + a_{k-1} p^{k-j-1} + \cdots + a_j$$
$$\left\lfloor \frac{r}{p^j} \right\rfloor = b_k p^{k-j} + b_{k-1} p^{k-j-1} + \cdots + b_j$$
$$\left\lfloor \frac{n-r}{p^j} \right\rfloor = c_k p^{k-j} + c_{k-1} p^{k-j-1} + \cdots + c_j$$

Hence $\left\lfloor \frac{n}{p^j} \right\rfloor - \left\lfloor \frac{r}{p^j} \right\rfloor - \left\lfloor \frac{n-r}{p^j} \right\rfloor = 1$ if and only if

$$\sum_{i=j}^{k} a_i p^i - \sum_{i=j}^{k} b_i p^i - \sum_{i=j}^{k} c_i p^i = p^j.$$

Subtracting this from

$$\sum_{i=0}^{k} a_i p^i - \sum_{i=0}^{k} b_i p^i - \sum_{i=0}^{k} c_i p^i = 0$$

we get

$$p^j + \sum_{i=0}^{j-1} a_i p^i = \sum_{i=0}^{j-1} b_i p^i + \sum_{i=0}^{j-1} c_i p^i,$$

i.e. in base p,

$$\overline{1a_{j-1}\dots a_1a_0} = \overline{b_{j-1}\dots b_1b_0} + \overline{c_{j-1}\dots c_1c_0}.$$

We have just proved the following amazing result.

Theorem 6. *The exponent of p in $\binom{n}{r}$ is equal to the number of carries when adding r and $n-r$ in base p.*

This result was proved by Kummer in 1852 [3]. Here are some straightforward consequences.

1. $\binom{m+n}{m}$ is odd if and only if, for each i, the ith binary digit of m or n is 0.
2. p divides $\binom{p^k+n}{n}$ if and only if $n \geq p^k(p-1)$.
3. p divides $\binom{p^k-1+n}{n}$ if and only if p^k does not divide n.

Many propoerties of the Sierpinski triangle can also be deduced from our discussion so far. But I should better stop and not ruin the fun for you!

References

[1] Wikipedia, *Factorial*, http://en.wikipedia.org/wiki/Factorial

[2] Wikipedia, *Sierpinski triangle*, http://en.wikipedia.org/wiki/Sierpinski_triangle

[3] Wikipedia, *Binomial coeficient*, http://en.wikipedia.org/wiki/Binomial_coefficient#Divisibility_properties