Three Short and Beautiful Proofs

Ted Szylowiec

1 Number theory

> *Fermat numbers, $F(n) = 2^{2^n} + 1$, are coprime to each other.*

Two numbers m and n are coprime if they have no factors in common except 1. In other words, if m and n are coprime then $(m,n) = 1$, where (m,n) is the greatest common divisor of m and n. We want to show that $F(n)$ is coprime to all the previous Fermat numbers

$$F(0),\ F(1),\ \ldots,\ F(n-1).$$

Instead of testing each of these individually, take the product of all of them:

$$P(n-1) = \prod_{k=0}^{n-1} F(k).$$

Now, if we can show that $(F(n),\, P(n-1)) = 1$ then we have shown that $F(n)$ has no factor in common with any of the Fermat numbers that make up $P(n-1)$. Look at the form of $P(n-1)$:

$$P(n-1) = (2^{2^{n-1}} + 1)\cdots(2^4+1)(2^2+1)(2+1).$$

Something very interesting happens when we multiply the right hand side by $(2-1)$, which we can do, since $(2-1)$ is just another way of writing 1. The factors in the product collapse into a simple form by repeatedly applying the algebra rule for the difference of two squares:

$$\begin{aligned} P(n-1) &= (2^{2^{n-1}} + 1)\cdots(2^{2^2}+1)(2^{2^1}+1)(2+1)(2-1) \\ &= (2^{2^{n-1}} + 1)\cdots(2^{2^2}+1)(2^{2^1}+1)(2^{2^1}-1) \\ &= (2^{2^{n-1}} + 1)\cdots(2^{2^2}+1)(2^{2^2}-1) \\ &\ \vdots \\ &= (2^{2^{n-1}} + 1)(2^{2^{n-1}} - 1) \\ &= 2^{2^n} - 1. \end{aligned}$$

This can be written in terms of $F(n)$:

$$P(n-1) = F(n) - 2. \tag{1}$$

Suppose that $F(n)$ and $P(n-1)$ have a factor q in common. If q divides $F(n)$ and q divides $P(n-1)$ then according to (1), q divides 2. Therefore the only possible values for q are 1 and 2. But Fermat numbers are all odd, so q cannot be 2. Therefore we have

$$(F(n),\, P(n-1)) = 1$$

The Fermat number $F(n)$ is coprime to all previous Fermat numbers. Since n can be anything, any Fermat number is coprime to all others.

2 Combinatorics

> *If $a+b+c+d+\cdots$ has m terms, then the maximum coefficient in the expansion of*
>
> $$(a+b+c+d+\cdots)^n$$
>
> *is*
>
> $$\frac{n!}{(q!)^m(q+1)^r}$$
>
> *where q is the quotient of n/m and r is the remainder.*

The coefficent of the term

$$a^{n_1}b^{n_2}c^{n_3}\cdots$$

where $n_1 + n_2 + \cdots + n_m = n$, is given by the multinomial

$$\frac{n!}{n_1!n_2!\cdots n_m!}. \tag{2}$$

This coefficient is largest when the denominator is as small as possible. Because factorials grow so fast, this can only happen when each of the m numbers n_1, n_2,... are as close to each other as possible. Before we go on we should make this more precise and give an argument as to why it should be so.

> *Let $n_1 + n_2 + \cdots + n_k = N$. Then $n_1!n_2!\cdots n_k!$ is smallest when $n_1 = n_2 \cdots = n_k$.*

Let $n_1 = n_2 \cdots = n_k = n$. We have $n_1!n_2!\cdots n_k! = (n!)^k$. Let's make a deviation in some of the n_i. We will make one larger by 1. If we do so, another n_i will have to be decreased by 1, so that the sum of the n_i remains N. We have:

$$\begin{aligned} (n+1)!\,(n-1)!\,(n!)^{k-2} &= (n+1)\,n!\,(n-1)!\,(n!)^{k-2} \\ &= (n+1)(n-1)!\,(n!)^{k-1}. \end{aligned}$$

But $(n+1)(n-1)! > n!$. Therefore

$$(n+1)!\,(n-1)!(n!)^{k-2} > (n!)^k.$$

A small deviation from equality gives a larger value for the product of factorials.

We must therefore find a way to either make all the n_i equal, or make them as close to each other as possible.

This is equivalent to a combinatorics problem: how can we distribute n balls into m boxes such that each box gets the same number of balls (or nearly)? Each box must have at least q balls, where q is the quotient of n/m. There may be balls left over. The remainder r must be distributed to r different boxes to ensure that the number of balls in two different boxes never differ by more than one. This is a fantastic way of thinking about Euclidean division. If there are n balls and m boxes then

$$n = qm + r, \quad 0 \le r < m$$

gives a way to distribute the balls so that each box has nearly the same number. The dividend is the number of balls, the divisor is the number of boxes, the quotient is the the number of balls each box gets initially, and the remainder is the number of boxes that must get an extra ball.

After we perform this distribution, m of the boxes will have q balls in them, and r of the boxes will have $q+1$ balls. Therefore we have

$$n_1!n_2!\cdots n_m! = q!\,q!\cdots q!\,(q+1)!\,(q+1)!\cdots(q+1)!$$

where there are m factors of $q!$ and r factors of $(q+1)!$. Putting this into (2) gives

$$\frac{n!}{q!^m (q+1)!^r}, \quad n = qm + r, \quad 0 \le r < m \tag{3}$$

It is instructive to see formula (3) in action. Suppose we want the maximum coefficient in the expansion of

$$(a+b+c)^8.$$

Here, $n = 8$ and $m = 3$. Euclidean division gives $q = 2$ and $r = 2$. In other words, 8 balls distributed into 3 boxes by putting 2 balls in one of them and 2+1 balls in the other two boxes. By (3),

$$\frac{8!}{(2!)^1(2+1)!^2} = 560.$$

Some further examples:

Expression	n	m	$n = qm + r$	Maximum
$(a+b)^{10}$	10	2	$10 = 5 \times 2 + 0$	252
$(a+b)^{11}$	11	2	$11 = 5 \times 2 + 1$	462
$(a+b+c+d)^9$	9	4	$9 = 2 \times 4 + 1$	7560

You can check these with a computer algebra system like `Maxima`[1] or `SageMath`[2].

3 Analysis

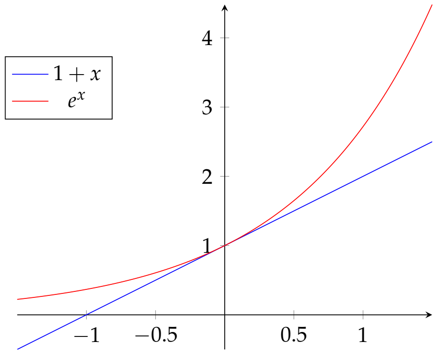
Let $a_1, a_2, \dots a_n \ge 0$ be n real numbers. Then

$$\sqrt[n]{a_1 a_2 \cdots a_n} \le \frac{a_1 + a_2 + \cdots + a_n}{n}. \tag{4}$$

This is called the Arithmetic-Geometric Mean inequality. It says that the geometric mean of n numbers is always less than or equal to the arithmetic mean. This is a very important inequality. Many problems can be solved by it. It pays to know a good way to prove it. The proof presented here is based on the one discovered by the Hungarian mathematician George Polya.

If one of the a_i is zero, then (4) is trivially true. So we consider only the case where $a_i > 0$.

The function e^x has the property that at any point x, the slope of the tangent to the curve $y = e^x$ is also e^x. Therefore at $x = 0$ the slope of the tangent line is $e^0 = 1$, and the equation of the tangent is $y = 1 + x$. Since e^x is convex and always greater than zero, it will remain above the tangent line.



From this argument we have established:

$$1 + x \le \exp(x). \tag{5}$$

Let A be the average of the a_i:

$$A = \frac{a_1 + a_2 + \cdots + a_n}{n}.$$

Since all the a_i are greater than zero, we have $A > 0$, and thus an x_k can be defined for every a_k like so:

$$x_k = \frac{a_k}{A} - 1.$$

Each x_k can be substituted into (5), giving n inequalities:

$$\frac{a_1}{A} \le \exp\left(\frac{a_1}{A} - 1\right)$$
$$\vdots$$
$$\frac{a_n}{A} \le \exp\left(\frac{a_n}{A} - 1\right).$$

Multiplying all these inequalities together,

$$\begin{aligned}
\frac{a_1 \cdots a_n}{A^n} &\le \exp\left(\frac{a_1}{A} - 1\right) \times \cdots \times \exp\left(\frac{a_n}{A} - 1\right) \\
&\le \exp\left(\frac{a_1}{A} - 1 + \frac{a_2}{A} - 1 + \cdots \frac{a_n}{A} - 1\right) \\
&\le \exp\left(\frac{a_1 + a_2 + \cdots + a_n}{A} - n\right) \\
&\le \exp(n - n)
\end{aligned}$$

finally gives

$$\frac{a_1 a_2 \cdots a_n}{A^n} \le 1$$

which is the same as (4).

A final thought: when does the equality hold? When is the arithmetic mean strictly equal to the geometric mean? If $a_1 = a_2 \cdots = a_n$ then each of the a_i are equal to the average value A. We then have $a_1 a_2 \cdots a_n = A^n$.

[1] Get `Maxima` here: `http://maxima.sourceforge.net`

[2] Get `SageMath` here: `http://www.sagemath.org/`