IMO Training Session March 21 2015 [1

T. J. LAFFEY NUMBER THEORY

We denote by $[x]$ the greatest integer $\leq x$. For example $\left[\frac{11}{3}\right] = 3, \left[\frac{15}{4}\right] = 3,$ $\left[\frac{16}{4}\right] = 4, \left[\frac{17}{4}\right] = 4.$

(1) Let n be a positive integer and p a prime number. We wish to find the greatest integer k for which p^k divides $n!$.

Example If $n = 17$, $17! = 17 \cdot 16 \cdot 15 \cdot 14 \cdot 13 \cdot 12 \cdot 11 \cdot 10 \cdot 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1$

$$k = \overset{16}{4} + \overset{14}{1} + \overset{12}{2} + \overset{10}{1} + \overset{8}{3} + \overset{6}{1} + \overset{4}{2} + \overset{2}{1}$$

$$= 15.$$

Note that in $n!$ written down as

$$1 \cdot 2 \cdot 3 \cdot \cdots \cdot (n-1) \cdot n$$

the last factor divisible by p is ap where $a = \left[\frac{n}{p}\right]$.

Now $n! = 1 \cdot 2 \cdot 3 \cdots n$

and the factors divisible by p are

$$1p, 2p, 3p, \ldots, ap, \text{ where } a = \left[\frac{n}{p}\right].$$

Take out the factor p from each of those to get a factor p^a of $n!$. We are then left with the factors

$$1, 2, 3, \ldots, a.$$

The multiples of p in this list are

$$1p, 2p, 3p, \ldots \left[\frac{a}{p}\right]p; \quad b = \left[\frac{a}{p}\right], \text{ say.}$$

These contribute a factor p^b of $n!$, leaving the factor

$$1 \cdot 2 \cdot 3 \cdots b.$$

Again the multiples of p here are

$$1p, 2p, \ldots, \left[\frac{b}{p}\right]p, \quad c = \left[\frac{b}{p}\right]$$

giving the factor p^c and leaving the product

$$1 \cdot 2 \cdot 3 \cdots c$$

and a further factor p^d where $d = \left[\frac{c}{p}\right]$,

and a new factor

$$1 \cdot 2 \cdot 3 \cdots d.$$

Proceed in this way until we reach a $\left[\frac{x}{p}\right]$ with $x < p$, so $\left[\frac{x}{p}\right] = 0$.

Note that $a = \left[\frac{n}{p}\right]$, $b = \left[\frac{n}{p^2}\right]$ (one knows that $n = ap + r$ where $0 \le r < p$

$= (pb + s)p + r$ where $a = bp + s$, with $0 \le s < p$

$= p^2 b + sp + r$ and $0 \le sp + r < p^2$,

so $\left[\frac{n}{p^2}\right] = b$.

Similarly $c = \left[\frac{n}{p^3}\right]$, $d = \left[\frac{n}{p^4}\right]$, ...

This proves

Theorem. The largest integer k for which p^k divides $n!$ is

$$k = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \cdots$$

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

$\left[\frac{17}{32}\right] = 0$

[For the example $n = 17$, $p = 2$,

$k = \left[\frac{17}{2}\right] + \left[\frac{17}{4}\right] + \left[\frac{17}{8}\right] + \left[\frac{17}{16}\right] + 0 \equiv$

$= 8 + 4 + 2 + 1$

$= 15.$]

(2) A variation of the formula.

Write n in base p, that is, write

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

where $r, a_0, a_1, \ldots, a_r$ are nonnegative integers with $a_i < p$ for all i, $a_r \neq 0$.

[Example 100 in base 3 is

$$100 = 1 + 2 \cdot 3^2 + 3^4$$

so $r = 4$, $a_0 = 1$, $a_1 = 0$, $a_2 = 2$, $a_3 = 0$, $a_4 = 1$ here.]

Notice that $\left[\frac{n}{p^l}\right] = 0$ for $l > r$. Also

$$\left[\frac{n}{p}\right] = a_1 + a_2 p + a_3 p^2 + \cdots + a_r p^{r-1}$$

$$\left[\frac{n}{p^2}\right] = a_2 + a_3 p + \cdots + a_r p^{r-2}$$

$$\left[\frac{n}{p^3}\right] = a_3 + \cdots + a_r p^{r-3}$$

$$\vdots$$

$$\left[\frac{n}{p^r}\right] = a_r$$

Hence $k = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \cdots$

$=$

$$k = a_1 + a_2(1+p) + a_3(1+p+p^2) + \cdots + a_r(1+p+\cdots+p^{r-1})$$

$$= a_1 + \frac{a_2(p^2-1)}{(p-1)} + \frac{a_3(p^3-1)}{(p-1)} + \cdots + \frac{a_r(p^r-1)}{p-1}$$

$$= \frac{a_1(p-1) + a_2(p^2-1) + a_3(p^3-1) + \cdots + a_r(p^r-1)}{p-1}$$

$$= \frac{a_1 p + a_2 p^2 + a_3 p^3 + \cdots + a_r p^r - (a_1 + a_2 + a_3 + \cdots + a_r)}{p-1}$$

$$= \frac{a_0 + a_1 p + a_2 p^2 + a_3 p^3 + \cdots + a_r p^r - (a_0 + a_1 + a_2 + a_3 + \cdots + a_r)}{p-1}$$

$$= \frac{n - \sum_{i=0}^{r} a_r}{p-1} .$$

This is a useful formula and is often used in the solution of IMO questions.

Since $\sum_{i=0}^{r} a_r \geq 1$ as n is a positive integer, $k \leq \frac{n-1}{p-1}$, with equality if and only if $\sum_{i=0}^{r} a_r = 1$, that is $a_r = 1$ and the other $a_i = 0$ (since $a_r \neq 0$) and $n = p^r$. In particular, if $p = 2$,

$k \leq n-1$, with equality occurring precisely when n is a power of 2. In particular 2^n does not divide $n!$.

---

(3) Some IMO-type questions on number theory.

(1) (Australian Problem) A social group has n members, numbered $1, 2, 3, \ldots, n$. Members are encouraged to give gifts to other members. Some members give as a gift, a gift they had received from another member, so, to avoid the embarrassment of a member receiving as a gift a gift he had given to some member earlier, the group made the following rule: Member a can give a gift to member b only if n divides $a(b-1)$.
Prove that if all members obey the rule, the embarrassing scenario cannot occur.

Solution. Suppose for the sake of contradiction we have a chain

$$a_1 \to a_2 \to a_3 \to \cdots \to a_r \to a_1$$

where a_1 gives a gift to a_2, who gives it to a_3, - - , who gives it to a_r, whose gives it to a_1. Here $a_1, a_2, \cdots, a_r$ are distinct.

So n divides $a_1(a_2-1)$, $a_2(a_3-1)$, $\cdots$, $a_r(a_1-1)$.

Notice that if $r = 2$, then n divides $a_1(a_2-1) - a_2(a_1-1) = a_1 - a_2$.

But $1 \le a_1, a_2 \le n$, so n dividing $a_1 - a_2$ implies $a_1 = a_2$, which is nonsensical.

Suppose $r > 2$.

Notice that n dividing $a_1(a_2-1)$ and $a_2(a_3-1)$ and

$$(a_1a_3 - a_1) = (a_1a_2)a_3 - a_1 + \alpha a_3$$
$$= a_1(a_2a_3) - a_1 + \alpha a_3$$
$$= a_1a_2 - a_1 + \alpha a_3 + \beta a_1$$

is a multiple of n (where $\alpha = -a_1a_2 + a_1$, $\beta = -a_2a_3 + a_2$).

But now $a_1a_3 - a_1$ and $a_3a_4 - a_3$ divisible by n implies $a_1a_4 - a_1$ is divisible by n

Processing thus, we eventually obtain that $a_1 a_r - a_1$ is divisible by n. But then we get a contradiction as in the case $r = 2$.

(2) (Another Australian Problem). Let $n \geq 2$ be an integer. Prove that the polynomial equation

$$f(x) := 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots + \frac{x^n}{n!} = 0$$

has no integer roots.

Solution. When $n = 2$, the roots of

$$1 + x + \frac{x^2}{2} = 0$$

are not real, so the result holds.

Suppose $n > 2$ and that the equation has an integer root α. Note $\alpha \neq 0$, $\alpha \neq 1$.

Claim $\alpha \neq -1$.

Note that $\left| -\frac{1}{3!} + \frac{1}{4!} - \frac{1}{5!} + \cdots + \frac{(-1)^n}{n!} \right|$

$$\leq \frac{1}{3!} + \frac{1}{4!} + \frac{1}{5!} + \cdots$$

$$< \frac{1}{2^2} + \frac{1}{2^3} + \frac{1}{2^4} + \cdots = \frac{1}{2}$$

So $1 - 1 + \frac{1}{2!} - \frac{1}{3!} + \frac{1}{4!} \cdots + \frac{(-1)^n}{n!} > 0$.

This proves the Claim.

Hence α is divisible by a prime p.

On the expression

$$1 + \alpha + \frac{\alpha^2}{2!} + \frac{\alpha^3}{3!} + \cdots + \frac{\alpha^n}{n!}$$

note that in each term $\frac{\alpha^k}{k!}$ $(1 \leq k \leq n)$, p^k divides the numerator α^k and p^k does not divide $k!$ (as proved earlier). So in its lowest form $\frac{\alpha^k}{k!} = \frac{p a_k}{b_k}$ where a_k, b_k are integers with b_k not divisible by p.

Hence $\alpha + \frac{\alpha^2}{2!} + \frac{\alpha^3}{3!} + \cdots + \frac{\alpha^n}{n!} = \frac{pu}{v}$, where u, v are integers and p does not divide v. Hence $\frac{pu}{v} \neq -1$, contradicting the fact that α is a root of $f(x) = 0$. This proves the result.

[Schur proved that $f(x)$ cannot be factored as a product of two polynomials with rational coefficients and degree at least one, but the proof is more difficult than for simply showing $f(x)$ has no integer roots. Gauss's Lemma and the fact that $n! \cdot f(x) = x^n + n x^{n-1} + \cdots + n! x + n!$ has integer coefficients and the coefficient of x^n is 1 implies that if $f(x) = 0$ had a rational root, then it would have an integer root. So our proof implies $f(x) = 0$ has no rational roots].

(3) (Belgian Problem). Prove that there are infinitely many positive integers n such that the largest prime factor of $n^4 + n^2 + 1$ is equal to the largest prime factor of $(n+1)^4 + (n+1)^2 + 1$.

[11

IDEA: Factor $n^4+n^2+1 = n^4+2n^2+1-n^2$

$= (n^2+1)^2 - n^2 = (n^2-n+1)(n^2+n+1)$.

$\gcd(n^2-n+1, n^2+n+1) = 1$, since $n^2-n+1 = n(n-1)+1$ is odd, and if d divides n^2-n+1 and n^2+n+1, then d divides their difference $2n$, so d divides n (since d is odd) and thus d divides n^2-n and also n^2-n+1, so d divides 1.

So the biggest prime dividing n^4+n^2+1 is the biggest prime dividing n^2-n+1 or the biggest prime dividing n^2+n+1, and these primes are different.

Then $(n+1)^4+(n+1)^2+1 = \left((n+1)^2-(n+1)+1\right)\left((n+1)^2+(n+1)+1\right)$

$= (n^2+n+1)\left((n+1)^2+(n+1)+1\right)$.

So it is sufficient to show that for infinitely many positive integers n, the biggest prime dividing n^2+n+1 is bigger than the biggest prime dividing n^2-n+1 and the biggest prime dividing $(n+1)^2+(n+1)+1$.

(Note that $\gcd(n^2-n+1, (n+1)^2+(n+1)+1) =$
$\gcd(n^2-n+1, n^2+3n+3) = \gcd(n^2-n+1, 4n+2)$

$= \gcd(n^2-n+1,\ 2n+1)$ (since n^2-n+1 is odd)

But $2(n^2-n+1) = n(2n+1) - 3n + 2$ and

$2(3n-2) - 3(2n+1) = -7$. So

$\gcd(n^2-n+1,\ (n+1)^2+(n+1)+1) = 1$ or 7].

Let p_n be the greatest prime dividing n^2+n+1 and let $S = \{n \mid p_{n-1} < p_n$ and $p_n > p_{n+1}\}$.

We want to prove S is infinite.

Suppose for the sake of contradiction that S is finite and let M be its maximum element.

Then if $n > M$, $p_n < p_{n+1}$ or $p_n < p_{n-1}$.

Notice that p_{n^2} is either p_n or p_{n-1}, and therefore we can find for given $m > M$, an $n > m^4$ with $p_n > p_{n+1}$, and then $p_{n-1} > p_n$, $p_{n-2} > p_{n-1}$, $p_{n-3} > p_{n-2}, \cdots, p_m > p_{m+1}$, otherwise one of the numbers $m, m+1, \cdots, n$ is in S, giving a contradiction.

But then $p_m > p_n + n - m - 1 > m^4 - m$, while $p_m \le m^2+m+1$, giving $m^4 < (m+1)^2$

which is false.

This contradiction shows that S contains an element $q > M$, contrary to the definition of M. So the result holds.

(4) (Estonian Problem).

Let f be a non-constant function from the set of positive integers to itself satisfying the condition

$$a - b \text{ divides } f(a) - f(b)$$

for all positive integers a and b with $a \neq b$.

Prove that there are infinitely many primes p such that p divides $f(c)$ for some positive integer c (depending on p).

Solution. Suppose for the sake of contradiction that the set of such primes is finite, say $p_1, p_2, \cdots, p_m$. This means that for every positive integer k, $f(k)$ is a product of powers of $p_1, \cdots, p_m$

Let $f(1) = p_1^{a_1} p_2^{a_2} \cdots p_m^{a_m}$, where $a_1, a_2, \cdots$ a_m are nonnegative integers.

Let $l_1, \cdots, l_m$ be positive integers with $l_i > a_i$ $(i = 1, 2, \cdots, m)$ and let $a = p_1^{l_1} p_2^{l_2} \cdots p_m^{l_m}$.

By hypothesis, a divides $f(a+1) - f(1)$.

But $f(a+1) = p_1^{b_1} p_2^{b_2} \cdots p_m^{b_m}$, for some nonnegative integers $b_1, \cdots, b_m$.

Now $p_i^{l_i}$ divides $p_1^{b_1} p_2^{b_2} \cdots p_m^{b_m} - p_1^{a_1} p_2^{a_2} \cdots p_m^{a_m}$ and $l_i > a_i$ and this is impossible unless $b_i = a_i$.

Hence $f(a+1) = f(1)$.

Let b be a positive integer.

Then

$a+1-b$ divides $f(a+1) - f(b)$,

so $a+1-b$ divides $f(1) - f(b)$.

But there are infinitely many such a, since we can choose $b_1, \ldots, b_n$ arbitrarily subject to $b_i > a_i$ for all i.

Hence $f(b) = f(1)$, for all positive integers b. But this says that f is a constant function, contradicting the hypotheses.

So the given set of primes is infinite.

A well-known result related to this problem is: If $f(x)$ is a polynomial with integer coefficients and degree at least one, then there are infinitely many primes p for which p divides $f(c)$ for some integer c.

Note that if

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n$$

and a, b are integers, then

$$f(a) - f(b) = a_1(a-b) + a_2(a^2-b^2) + \cdots + a_r(a^r - b^r)$$

and $a^r - b^r = (a-b)(a^{r-1} + a^{r-2}b + \cdots + ab^{r-2} + b^{r-1})$

for every positive integer r.

So $a-b$ divides $f(a) - f(b)$, if $a \neq b$.

If $f(x) = 0$ for some nonnegative integer x, then clearly, given any prime p, there is a positive integer c such that p divides $f(c)$. [If $f(0) = 0$, take $c = p$; if $f(h) = 0$ for some $h > 0$, take $c = h$].

Assuming $f(x) \neq 0$ for all nonnegative integers x, then $|f|$ satisfies the conditions of Problem 4.

This is a proof of the quoted result.