LCD MATHEMATICS ENRICHMENT PROGRAMME 2014
Lecture on Number Theory February 8. T. J. LAFFEY

Kevin Hutchinson presented Euclid's proof that there are infinitely many prime numbers. It relies on the fact that if $n > 1$ is an integer, then n is the product of primes.

To recall Euclid's proof, suppose we have a finite number of primes $q_1, q_2, \cdots, q_m$. Form the number $M = q_1 q_2 q_3 \cdots q_m + 1$. Note that $M > 1$, so M is divisible by some prime p. But p is not any of the primes $q_1, q_2, \cdots, q_m$.

Variations of Euclid's proof are used to prove other results on primes.

Suppose $p > 3$ is a prime. Then on division by 3, p leaves remainder 1 or remainder 2.

Let X be the set of all primes $p > 3$ which leave remainder 1 on division by 3 and Y the set of all primes $p > 3$ which leave remainder 2 on division by 3.

We now prove

Proposition Y is infinite.

Proof Suppose for the sake of contradiction that Y is finite. Suppose $Y = \{l_1, l_2, \cdots, l_r\}$.

Form the number $T = 3 l_1 l_2 \cdots l_r + 2$.

Note that $T > 1$, so T is a product of primes. Let p be a prime dividing T. Note that $p \neq 2$, $p \neq 3$, and that p is not in Y. Hence $p \in X$. So $p = 3b+1$ for some integer b. Hence T is the product $(3b_1+1)(3b_2+1)\cdots(3b_t+1)$ for some $t \geq 1$, and integers $b_1, b_2, \cdots, b_t$. But notice that $(3x+1)(3y+1) = 3z+1$ where $z = 3xy + x + y$ and z is an integer if x and y are integers. Using this repeatedly, we get that $T = 3q+1$ for some integer q. Thus $3l_1l_2\cdots l_r + 2 = 3q + 1$ and thus $3(l_1l_2\cdots l_r - q) = -1$. But this says that 3 divides -1, as $l_1l_2\cdots l_r - q$ is an integer and this is a contradiction. So the Proposition is proved.

Dirichlet's Theorem is a vast generalization of this.

About 200 years ago, there was great interest in Mathematics, particularly in number theory. The German Mathematician C. F. Gauss, French Mathematicians Lagrange, Legendre and Swiss/Russian Mathematician Euler were interested in the function $\pi(x)$ which is defined to be the number of distinct primes $p \leq x$. So $\pi(2) = 1$, $\pi(10) = 4$, $\pi(20) = 8$. They wanted to know how $\pi(x)$ compares with other functions arising in algebra and calculus.

Legendre and Gauss both noticed that $\pi(x)$ and $\frac{x}{\ln(x)}$ are closely related for many x.

Nowadays with the help of computers it is easy to find $\pi(x)$ for fairly large numbers, for example, $\pi(10^{14}) = 3,204,941,750,802$ while $10^{14}/\ln(10^{14}) \doteq 3,102,103,442,166$, and the ratio $\frac{\pi(x)}{(x/\ln(x))}$ is approximately 1.03 for $x = 10^{14}$.

It was conjectured that as $x \to \infty$, the ratio $\frac{\pi(x)}{(x/\ln(x))} \to 1$ ⊛

This was proved about 80 years after it was conjectured. In 1896, Hadamard (a very famous French mathematician) and de la Vallée Poussin, (a very famous Belgian mathematician) independently proved ⊛. The result is called the Prime Number Theorem.

When it was first conjectured, no progress on proving it was made for some time. The first person to make substantial progress was the Russian mathematician Chebyshev.

The binomial theorem states that for a positive integer n,

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

where $\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{n(n-1)\cdots(n-k+1)}{k!}$ is

the number of ways of choosing a team of k players from n players, so $\binom{n}{k}$ is an integer.

Chebyshev considered the expansion

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

First one checks that $\binom{2n}{n}$ is the biggest coefficient occurring.

Putting $x=1$ and noting that there are $2n+1$ terms, the first and last being 1, we get

$$(2n-1)\binom{2n}{n} \geq (1+1)^{2n} - 2 = 4^n - 2,$$

So $$\binom{2n}{n} \geq \frac{4^n-2}{2n-1} \geq \frac{4^n}{2n} \text{ (check).}$$

Notice that $\binom{2n}{n} < 4^n$. Now $\binom{2n}{n} = \frac{(2n)!}{(n!)^2}$

$$= \frac{2n(2n-1)(2n-2)\cdots(n+1)}{1\cdot 2\cdot 3\cdots n}$$ and notice that any prime p with $n+1 \leq p \leq 2n$ occurs only in the top of the fraction as all the factors in the bottom are smaller than p. Hence p divides $\binom{2n}{n}$.

Now $\pi(2n) - \pi(n)$ is the number of primes p with $n+1 \leq p \leq 2n$, so it follows that $\binom{2n}{n}$ is divisible by the product of them all and thus

$$n^{\pi(2n)-\pi(n)} \leq \binom{2n}{n} < 4^n$$

Taking logs one gets

$$\pi(2n) - \pi(n) \leq \frac{n\ln(4)}{\ln(n)}.$$

One can show that if p is a prime and k the biggest integer for which p^k divides $\binom{2n}{n}$, then $p^k \leq 2n$.

Since any prime dividing $\binom{2n}{n}$ is at most $2n$, one deduces that

$$(2n)^{\pi(2n)} \geq \binom{2n}{n} \geq \frac{4^n}{2n}$$

and taking logs

$$\pi(2n) \geq \frac{n \ln(4)}{\ln(2n)} - 1.$$

Another result of Chebyshev deals with the function $\gamma(n)$ = product of all the primes dividing n, for given positive integer $n > 1$.

Consider for a positive integer m,

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

and $\binom{2m+1}{m+1} = \binom{2m+1}{m}$. Hence

$$\binom{2m+1}{m+1} < 2^{2m}.$$

But $\binom{2m+1}{m+1} = \dfrac{(2m+1)(2m)\cdots(m+2)}{1 \cdot 2 \cdot 3 \cdots m} \geq \dfrac{\gamma(2m+1)}{\gamma(m+1)}$

since primes $p > m+1$ appear in the top and do not cancel. Hence

$$\frac{\gamma(2m+1)}{\gamma(m+1)} < 2^{2m}.$$

Proposition. Let $n > 1$ be an integer. Then
$$\gamma(n) < 2^{2n}.$$

Proof $\gamma(2) = 2$, so the result holds for $n = 2$.

Using complete induction, assume $n > 2$ and that $\gamma(k) < 2^{2k}$ for all k with $2 \leq k \leq n-1$.

We try to deduce that $\gamma(n) < 2^{2n}$.

If n is even, then, since $n > 2$, n is not prime and $\gamma(n) = \gamma(n-1) < 2^{2(n-1)} < 2^{2n}$, as required. Suppose then that n is odd.

Write $n = 2m+1$ and note that $m+1 < n$.

Now $\gamma(n) = \gamma(2m+1) < 2^{2m}\gamma(m+1)$
$$< 2^{2m} \cdot 2^{2(m+1)} = 2^{2(2m+1)} = 2^{2n},$$
as required. So the induction step is established and the proof is complete. ∎

Bertrand around 1850 conjectured that if $n > 1$ is an integer, then there exists a prime p with $n < p < 2n$.

Bertrand checked his conjecture for n up to 30,000 but could not prove it in general. Chebyshev proved it using the above proposition.

Legendre conjectured that if n is a positive integer, there must be a prime p with $n^2 < p < (n+1)^2$.

This is still not proved but great progress has been made recently.

Mathematical Enrichment Programme 2014

Some factorizations and formulae

1) For a positive integer n,
$$a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + a^{n-3}b^2 + \cdots + ab^{n-2} + b^{n-1}).$$

2) For an odd positive integer n,
$$a^n + b^n = (a+b)(a^{n-1} - a^{n-2}b + a^{n-3}b^2 - \cdots - ab^{n-2} + b^{n-1}).$$

3) $x^3 + y^3 + z^3 - 3xyz = (x+y+z)(x^2+y^2+z^2-xy-yz-zx)$.

4) $(x+y+z)^3 - x^3 - y^3 - z^3 = 3(x+y)(y+z)(z+x)$.

5) $x^4 + 4 = x^4 + 4x^2 + 4 - 4x^2 = (x^2+2)^2 - (2x)^2$
$= (x^2 - 2x + 2)(x^2 + 2x + 2)$.

6) $x^4 + x^2y^2 + y^4 = x^4 + 2x^2y^2 + y^4 - (xy)^2 = (x^2 - xy + y^2)(x^2 + xy + y^2)$.

7) $(x+y)^5 - x^5 - y^5 = 5xy(x+y)(x^2 + xy + y^2)$.

8) $(x+y)^7 - x^7 - y^7 = 7xy(x+y)(x^2 + xy + y^2)^2$.

9) Binomial Theorem
$$(1+x)^n = 1 + \binom{n}{1}x + \binom{n}{2}x^2 + \cdots + \binom{n}{n}x^n,$$
where $\binom{n}{k} = \dfrac{n!}{k!\,(n-k)!} = \dfrac{n(n-1)\cdots(n-k+1)}{k!}$,

$0! = 1$.

10) The roots of the equation $z^n = 1$ in the complex numbers are $\cos\left(\frac{2\pi k}{n}\right) + i\sin\left(\frac{2\pi k}{n}\right)$, $k = 0, 1, 2, \cdots, (n-1)$.

11) For positive integer n and prime p, the largest integer k for which p^k divides $n!$ is
$$k = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \cdots = \sum_{\ell=1}^{\infty}\left[\frac{n}{p^\ell}\right].$$
Here $[x]$ is the greatest integer not exceeding x.
[For example, with $n = 100$ and $p = 7$,
$k = \left[\frac{100}{7}\right] + \left[\frac{100}{7^2}\right] + \left[\frac{100}{7^3}\right] + \cdots = 14 + 2 + 0 = 16$]

(12) If p is a prime and p^m divides $\binom{2n}{n}$, then $p^m \leq 2n$.

· Square bracket function : x a real number.

$[x]$ denotes the greatest integer $\leq$ not exceeding x. [1]

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

$[4] = 4$, $[4.37] = 4$, $[-1.6] = -2$.

If a, b are positive integers, we can write

$$a = bq + r$$

where $q \geq 0$ and r are integers with $0 \leq r < b$.

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

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

Factorization and Formulae Sheet ; Formulae (1) to (8) can be proved by direct multiplication.

Formula 11. Let n be a positive integers and p a prime. We want to find a formula for the greatest integer k for which p^k divides $n!$.

Solution: List the numbers

$$1, 2, 3, \cdots, n$$

Pick out the multiples of p in the list

$$1p, 2p, 3p, \cdots, ap \qquad a = \left[\frac{n}{p}\right]$$

We get an obvious factor p^a from the product of these. We now look for extra powers of p from the product of

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

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 products 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

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

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

Notice that this can be written

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

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

A variation on 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 $a_0, a_1, \cdots, a_r$ are integers with $0 \le a_j \le p-1$ for all j and $a_r \neq 0$.

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

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

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

so $k < n$. Hence p^n does not divide $n!$.

Formula 12 on sheet.

The highest powers 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 $s \leq t$ and thus

$p^s \leq p^t \leq 2n$.

Exercises

1. For an integer $k > 1$, let $\lambda(k)$ be the sum of the primes dividing k. [So, for example, $\lambda(60) = 2+3+5 = 10$].
Call an integer $n > 2$ peculiar if
$$\lambda(n) + 1 = \lambda(n-1).$$
Prove that 2014 is peculiar.

2. Find with proof all integers k for which $4k^4 + 1$ is a prime number.

3. Let $\{p_n\}$ be the (increasing) sequence of prime numbers, so $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7$, ...
Suppose that $k > 3$ is an integer with $p_{k+1} - p_k = 2$. Prove that $p_{k+2} - p_{k+1} \neq 2$.
[Hint: Consider remainders on division by 3].