Mathematics Enrichment Programme 2016.
UCD. February 13 2016
T. J. Laffey

1. Some basic number theory.

$\mathbb{Z} = \{0, 1, -1, 2, -2, 3, -3, \cdots\}$

is the set of integers

$\mathbb{N} = \{1, 2, 3, 4, \cdots\}$

is the set of positive integers; also called the set of natural numbers.

If a, b are integers and $b \neq 0$, we say that b divides a if $a = bc$ for some integer c.

Long division: Suppose a, b are integers and $b \neq 0$. Then we can find integers q, r with $a = bq + r$ with $0 \leq r < |b|$.

q is called the quotient and r the remainder of a on division by b.

Example $a = 100$, $b = 7$, $100 = 14 \times 7 + 2$, so $q = 14$ and $r = 2$.

Prime Numbers.

An integer $p > 1$ is prime if the only positive integers that divide p are 1 and p. [2

The sequence of primes is
$2, 3, 5, 7, 11, 13, 17, 19, 23, \ldots$

Fundamental Theorem of Arithmetic: Suppose $n > 1$ is an integer. Then n is a product of prime numbers. Furthermore, the expression of n as a product of primes is unique up to the order of the factors.

Example $60 = 2 \times 2 \times 3 \times 5 = 2 \times 5 \times 3 \times 2$
$= 5 \times 2 \times 2 \times 3 = \cdots$, but there is no way to write 60 as a product of primes except to use two 2s, one 3 and one 5.

Important Consequence: Suppose that a and b are integers and p a prime. Suppose p divides ab. Then p divides a or p divides b (or both).

Infinitude of primes: Theorem.

There are infinitely many prime numbers.

The largest known prime number at present is $2^{74207281} - 1$.

It has 22,338,618 digits. It was found last year by Curtis Cooper of the University of Central Missouri. The proof that it is prime took 31 days on a PC with an Intel i7-4790 CPU.

Proofs that there are infinitely many primes.

The most famous one is due to Euclid around 2500 years ago:

Suppose there are only finitely many primes. Call them $q_1, q_2, \cdots, q_k$.

Let $N = q_1 q_2 \cdots q_k + 1$. Clearly $N > 1$ and it is an integer, so it is a product of primes. Let p be a prime dividing N. Note that none of the primes $q_1, q_2, \cdots, q_k$ divide N – in fact, they each leave a remainder 1 when divided into N. So p is not one of these. But $q_1, q_2, \cdots, q_k$ is the full list of primes. Contradiction.

A variant of Euclid's proof.

Suppose that there are only finitely many primes and let p be the biggest one and let $N = p! + 1$. If q is any prime, then $q \leq p$, so q divides $p!$, so q does not divide $p! + 1 = N$. So N is not divisible by any prime Contradiction.

Goldbach's proof (1760)

For a natural number n, let $F_n = 2^{2^n} + 1$.
So $F_1 = 2^2 + 1 = 5$, $F_2 = 2^4 + 1 = 17$, $F_3 = 2^8 + 1 = 257$, $F_4 = 2^{16} + 1 = 65537$, ...

Observe that for $n > 1$,

$$F_n = 2 + F_1 F_2 \cdots F_{n-1} \quad \ldots (1)$$

To see this, note that $F_n - 2 = 2^{2^n} - 1$

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

and $2^{2^{n-1}} - 1 = (2^{2^{n-1}} + 1) - 2 = F_{n-1} - 2$.

Using proof by induction, we may assume that $F_{n-1} - 2 = F_1 F_2 \cdots F_{n-2}$

But now ② gives $F_n - 2 = F_1 F_2 \cdots F_{n-2} F_{n-1}$, proving the result.

Let p be a prime dividing F_n. Then by (1), p does not divide any of the numbers $F_1, F_2, \cdots, F_{n-1}$.

Hence $\gcd(F_r, F_s)$ for all positive integers r, s with $r \neq s$.
Let l_n be a prime divisor of F_n.
Then $l_1, l_2, l_3, \ldots$ is a list of distinct primes, so there are infinitely many primes.

Testing if a given integer $n > 1$ is prime.

For $n > 1$ a non-prime, we know that $n = q_1 q_2 \cdots q_r$ for some $r \geq 2$ and primes $q_1, q_2, \ldots, q_r$. So $n \geq p^2$, where p is the least of the q_i's. So n is divisible by a prime $p \leq \sqrt{n}$.

So to test if a given n is a prime one can make a list of all primes $p \leq \sqrt{n}$ and check if any of them divides n. If not, then n is prime.

Example 1. $n = 199$, $\sqrt{n} < 15$, and one checks that n is not divisible by $2, 3, 5, 7, 11, 13, 17$ or 19. So n is prime

Example 2 $n = 323$. $n < 18^2 = 324$, so make list $2, 3, 5, 7, 11, 13, 17$ and one finds 17 divides n. So $n = 17 \times 19$.

What proportion of the integers 1, 2, ⋯, n are prime?

—

Suppose we know the first m primes, $p_1 = 2$, $p_2 = 3$, ---, p_m, say. Copying Euclid, let $M = p_1 p_2 \cdots p_m + 1$ and note that M is not divisible by any of the primes $p_1, p_2, \cdots, p_m$. Let l be a prime dividing M. Then $l \leq M$ and the $(m+1)^{st}$ prime p_{m+1} (in ascending order) must satisfy $p_{m+1} \leq l$.

So $p_{m+1} \leq p_1 p_2 \cdots p_m + 1$.

Exercise 1. Use this and induction on m to show that the n^{th} prime p_n satisfies $p_n \leq 2^{2^n} - 2$, for $n = 1, 2, 3, \cdots$

—

The inequality in Exercise 1 is very weak. It is a consequence of the Prime Number Theorem that the n^{th} prime p_n is 'close to' $n \ln(n)$.

The Prime Number Theorem states that if $\pi(x)$ is the number of primes not exceeding x, then

$$\frac{\pi(x)}{x/\ln(x)} \longrightarrow 1$$

as $x \longrightarrow \infty$.

The theorem was proved (independently) by Hadamard and de la Vallëe-Poussin in 1896.

Number Theoretic Functions:

Let n be a positive integer and define $d(n)$ to be the number of positive integers which divide n.

Suppose $q_1, q_2, \dots, q_r$ are the distinct primes dividing n. We can factor

$$n = q_1^{a_1} q_2^{a_2} \cdots q_r^{a_r}$$

for some positive integers $a_1, \dots, a_r$

Every positive integer m dividing n is of the form

$m = q_1^{b_1} q_2^{b_2} \cdots q_r^{b_r}$ where $b_1, b_2, \cdots, b_r$ are integers with $0 \leq b_j \leq a_j$ for $j = 1, 2, \cdots, r$ and

by unique factorization theorem, different choices of b's give different m's. Since $b_j \in \{0, 1, \cdots, a_j\}$, we have $a_j + 1$ choices for b_j (independently of the choice of b_i $(i \neq j)$ so we have $(a_1 + 1)(a_2 + 1) \cdots (a_r + 1)$ choices in all. Thus

$$d(n) = (a_1+1)(a_2+1) \cdots (a_r+1).$$

Example $1000 = 10^3 = 2^3 \times 5^3$, so
$d(1000) = (3+1)(3+1) = 16$.

Exercise 2. Prove that the sum of all ~~the~~ positive divisors of n above is

$$\sigma(n) = \left(\frac{q_1^{a_1+1} - 1}{q_1 - 1}\right)\left(\frac{q_2^{a_2+1} - 1}{q_2 - 1}\right) \cdots \left(\frac{q_r^{a_r+1} - 1}{q_r - 1}\right).$$

A *perfect number* is a positive integer n such that the sum of all its positive divisors $\sigma(n) = 2n$.

Examples 6, 28, 496, 8128.

Exercise 3. Let p be a prime of the form $2^k - 1$ where k is a positive integer. (For example, $31 = 2^5 - 1$).

Prove that k is a prime.

Prove also that $p(p+1)/2$ is a Perfect number. (For example, when $k = 5$, we get the perfect number 496).

Exercise 4 (Hard problem). Prove that every *even* perfect number is of the form $p(p+1)/2$ where p is a prime of the form $2^k - 1$ (such a prime is called a *Mersenne* prime).

Remark. It is not known whether an odd perfect number exists.

The greatest integer function.

For a real number x, define $\lfloor x \rfloor$ to be the greatest integer not exceeding x

($\lfloor x \rfloor$ is often written as $[x]$ for ease of writing and typing).

Examples $[3]=3$, $[7/2]=3$, $[\pi]=3$, $[\sqrt{10}]=3$; $[\log_2 2016]=10$.

Prop. Let n be a positive integer. Then
$$[\sqrt{n^2+2n}]=n.$$

Proof $n^2 < n^2+2n < n^2+2n+1=(n+1)^2$,
so $n < \sqrt{n^2+2n} < n+1$.

Example. $[\sqrt{(3!)!}\,] = 26$.

Proposition. Let v and s be positive integers with $v \geq s$. The least number q for which it is impossible to partition v objects into $s+1$ subsets each having $\geq q$ elements is $\left[\frac{v}{s+1}\right]+1$.

Proof. If m is a positive integer $\leq \frac{v}{s+1}$, then $m(s+1) \leq v$ and we can split v objects into $s+1$ subsets of size m (with possibly some objects not used. But if m is an integer $> \frac{v}{s+1}$, then $m(s+1) > v$ and there are too few objects to create $s+1$ sets of size m without overlap.

The Proposition is relevant at present. In the election, if a constituency has s seats to fill and there are v valid votes cast, the quota q is the smallest integer for which it is impossible for $s+1$ candidates to each receive at least q first preference votes.

So $$q = \left[\frac{v}{s+1}\right] + 1.$$

For example, in a four seat constituency,
$$q = \left[\frac{v}{5}\right] + 1$$
where v is the number of valid votes cast.

PAST IMO Questions and Solutions

The website imo-official.org has a button Problems which enables one to get copies of the questions used in previous IMOs. Also, for some years, you can find there the list of all problems shortlisted for the competition together with the official solutions.

Solutions to the exercises

Exercise 1, page 6.

We use the method of complete induction. When $n=1$, $p_1 = 2$ and $2^{2^1}-2 = 2^2-2 = 2$, so the inequality is true for $n=1$. Assume the inequality holds for $n=1, \ldots, k$ and try to deduce that it holds for $n=k+1$. Now

$$
\begin{aligned}
p_{k+1} &\leq p_1 p_2 \cdots p_k + 1 \\
&\leq (2^2-2)(2^{2^2}-2) \cdots (2^{2^k}-2) + 1 \\
&\leq 2^2 \cdot 2^{2^2} \cdots 2^{2^{k-1}} (2^{2^k}-2) + 1 \\
&< 2^2 \cdot 2^{2^2} \cdots 2^{2^k} - 2 + 1 \\
&= 2^{2(2^k-1)} - 2 + 1
\end{aligned}
$$

(using the formula $2 + 2^2 + \cdots + 2^{2^k} = \dfrac{2(2^k-1)}{2-1}$ for summing the geometric progression)

But $2^{2(2^k-1)} = 2^{2^{k+1}-2} < 2^{2^{k+1}} - 1$.

Hence

$$p_{k+1} \leq 2^{2^{k+1}} - 1 - 2 + 1 = 2^{2^{k+1}} - 2.$$

So the inequality holds for $n = k+1$. So the result is proved by complete induction.

Exercise 2, page 7.

$\sigma(n)$ is the sum of all the positive integers which divide n. We prove the result in a few steps.

Step 1. Suppose $n = p^r$, where p is a prime and $r \geq 0$ is an integer. Then by the Fundamental Theorem of Arithmetic, the positive divisors of n are the powers p^s, ~~where~~ s is an integer, with $0 \leq s \leq r$.

So the sum of the divisors of n is

$$p^0 + p^1 + \cdots + p^r = \frac{p^{r+1} - 1}{p - 1} \quad \text{---(1)}$$

using the formula for the sum of a geometric progression.

Step 2. Suppose $n = ab$, where a, b are positive integers with $\gcd(a, b) = 1$. Suppose m is a positive integer which divides n. Since $\gcd(a, b) = 1$, there is no prime which divides both a and b. Hence, by the fundamental theorem of arithmetic again, $m = xy$, where x and y are positive integers such that x divides a and y divides b.

Now suppose that the number of positive integers, $d(a)$, which divide a, is k and that $d(b) = l$. Let $x_1, x_2, \dots, x_k$ be all the positive divisors of a and $y_1, y_2, \dots, y_l$ be all the positive divisors of b. Note that every product $x_i y_j$ $(i = 1, 2, \dots, k, j = 1, 2, \dots, l)$ divides ab and that all these products are distinct. [For suppose $x_i y_j = x_u y_v$ for some i, j, u, v with $(i, j) \neq (u, v)$.

By the uniqueness part of the fundamental theorem of arithmetic and the fact That x_i, x_u divide a and y_j, y_v divide b, so that x_i, x_u have no prime divisors in common with y_j, y_v (as $\gcd(a, b) = 1$), we find $x_i = x_u$, $y_j = y_v$, so $i = u, j = v$, which is a contradiction].

So all the products $x_i y_j$ are distinct, as claimed.

So the sum $\sigma(ab)$ of all the positive divisors of ab is:

$$\begin{array}{l} x_1y_1 + x_1y_2 + \cdots + x_1y_l + \\ x_2y_1 + x_2y_2 + \cdots + x_2y_l + \\ \qquad\vdots \qquad\qquad\qquad \vdots \\ \qquad\qquad\qquad\qquad\quad + \\ x_ky_1 + x_ky_2 + \cdots \qquad + x_ky_l \end{array}$$

$$= (x_1 + x_2 + \cdots + x_k)(y_1 + y_2 + \cdots + y_l]$$

$$= \sigma(a)\,\sigma(b).$$

So if $\gcd(a,b]=1$, then $\sigma(ab] = \sigma(a)\,\sigma(b)$ ... (2)

Final Step Let $n = q_1^{a_1} \cdots q_r^{a_r}$, where $q_1, \dots, q_r$ are distinct primes and $a_1, \dots, a_r$ positive integers. We prove the formula by induction on r.

If $r = 1$, $n = q_1^{a_1}$ and $\sigma(n] = \dfrac{q_1^{a_1+1} - 1}{q_1 - 1}$, using (1) above. So the formula holds if $r = 1$.

Assume the formula holds for $r-1$ and try to deduce it for r.

Take $a = q_1^{a_1} \cdots q_{r-1}^{a_{r-1}}$, $b = q_r^{a_r}$. Then $n = ab$ and since all the q_i are distinct primes, $\gcd(a, b) = 1$.

So, by the result of Step 2,

$$\sigma(n) = \sigma(ab) = \sigma(a)\,\sigma(b) = \underbrace{\left(\frac{q_1^{a_1+1}-1}{q_1-1}\right)\cdots\left(\frac{q_{r-1}^{a_{r-1}+1}-1}{q_{r-1}-1}\right)}_{\sigma(a)} \cdot \underbrace{\left(\frac{q_r^{a_r+1}-1}{q_r-1}\right)}_{\sigma(b)},$$

the formula for $\sigma(a)$ comes from the induction hypothesis, since a has only $r-1$ distinct prime divisors, and the formula for $\sigma(b)$ from (1) above.

So we have deduced that $\sigma(n)$ has the desired form. So the result is proved by induction.

(Example of the result). The sum of all the positive divisors of 2016.

$2016 = 2^5 \times 3^2 \times 7$, so

$$\sigma(2016) = \left(\frac{2^6-1}{2-1}\right)\left(\frac{3^3-1}{3-1}\right)\left(\frac{7^2-1}{7-1}\right) = 6552.$$

Exercise 3 $p = 2^k - 1$, where k is a positive integer. If $k = 1$, then $p = 2^1 - 1 = 1$ is not a prime.

Suppose $k > 1$ is not a prime. Say $k = ab$ where $a > 1$ and $b > 1$ are integers. Observe that

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

[The factorization $x^m - 1 = (x-1)(x^{m-1} + x^{m-2} + \cdots + x + 1)$ is proved by multiplying out the right-hand-side and cancelling terms. Take $x = 2^a$, $m = b$ to get the factorization of $2^{ab} - 1$ given here].

Since $a > 1$, $2^a - 1 \geq 3$ and since $b > 1$, the second factor is at least 5.

So $2^{ab} - 1$ is not prime.

Hence if p is prime, k must be prime. [A prime of the form $2^k - 1$ is called a Mersenne prime. Mersenne was a monk who discovered that one can find many primes of this form. A couple of hundred years later, the French mathematician Lucas discovered some properties of numbers of the form 2^n-1 and his work was extended by the American mathematician Lehmer to give a test for primality. By good fortune, it turned out that when computers were invented, it was found that the Lucas-Lehmer test could be run efficiently on a computer. That explains why the biggest known primes at present are Mersenne primes. Lucas without any computer or calculator succeeded in showing that $2^{127}-1$ (the case $k=7$) is prime and he held the record until the advent of fast computers.

Not all numbers 2^k-1 with k prime are prime. For example, $2^{11}-1 = 2047 = (23)(89)$ is not prime]

Second part of Exercise 3

Let $p = 2^k - 1$ be prime. Then $n = p(p+1)/2 = p\,2^{k-1}$ and p is odd, so, by the formula in Exercise 2, the sum of the positive divisors of n is $\sigma(n) = \left(\frac{p^2-1}{p-1}\right)\left(\frac{2^k-1}{2-1}\right)$

$= (p+1)\,(2^k-1) = (2^k)\,p = 2n,$

so n is a perfect number.

Exercise 4. Suppose n is a perfect even integer. We can write $n = 2^r s$ where $r \geq 1$ and $s \geq 1$ are integers and s is odd. Since n is perfect, $\sigma(n) = 2n$. Using the formula in Step 2 of Exercise 2 (with $a = 2^r$, $b = s$), we get

$$2^{r+1}s = 2n = \sigma(n) = \left(\frac{2^{r+1}-1}{2-1}\right)\sigma(s).$$

$$= (2^{r+1}-1)\,\sigma(s) \ldots \quad (1)$$

Now 2^{r+1} and $2^{r+1}-1$ differ only by 1, so $\gcd(2^{r+1}, 2^{r+1}-1) = 1$. So, by unique factorization, (1) implies that $2^{r+1}-1$ divides s.

We can write
$s = (2^{r+1}-1)s_0$, where s_0 is an integer. If $s_0 > 1$, then 1, $2^{r+1}-1$, s_0 and $(2^{r+1}-1)s_0$ are positive divisors of s and thus

$$\sigma(s) \geq 1 + 2^{r+1}-1 + s_0 + (2^{r+1}-1)s_0$$

$$> (s_0) + (2^{r+1}-1)s_0 = 2^{r+1}s_0$$

and thus

$$(2^{r+1}-1)\sigma(s) > (2^{r+1}-1)\,2^{r+1}s_0 = 2^{r+1}s,$$

since $s = (2^{r+1}-1)s_0$.

This contradicts equation (1).

Hence $s_0 = 1$ and $s = 2^{r+1}-1$.

But now (1) implies that

$$\sigma(s) = 2^{r+1}.$$

But $s = 2^{r+1}-1$ has divisors 1 and $2^{r+1}-1$ and these two sum to 2^{r+1}. Since $\sigma(s) = 2^{r+1}$, s has no other positive divisors. Hence $2^{r+1}-1$ is prime. Put $p = 2^{r+1}-1$. Then $n = 2^r s = 2^r p = p(p+1)/2$ and p is a Mersenne prime.