Perfect Numbers

Euler used the notation $\int n$ to denote the sum of the positive divisors of n – including n itself.

Example $\int 4 = 1+2+4 = 7$ $\int p = 1+p$ if p is prime

$\int 6 = 1+2+3+6 = 12$

Lemma If $\gcd(a,b) = 1$ for $a, b \in \mathbb{Z} \setminus \{0\}$, then

$$\int ab = \int a \int b$$

Proof The positive divisors of ab can each be written in the form $a_1 b_1$ where $a_1 | a$ and $b_1 | b$ $a_1, b_1 > 0$ in exactly one way

So $$\int ab = \sum_{\substack{c>0 \\ c|ab}} c = \Big(\sum_{\substack{a_1>0 \\ a_1|a}} a_1 \Big)\Big(\sum_{\substack{b_1>0 \\ b_1|b}} b_1 \Big)$$

Definition $n \in \mathbb{Z}_+$, $n \geq 2$ is perfect if $\int n = 2n$, that is, n is the sum of its proper (positive) divisors (not counting n).

Example $\int 6 = 12 = 2 \times 6$

$\int 28 = 1+2+4+7+14+28 = 56 = 2 \times 28$

$6 = 2 \times 3$ $28 = 4 \times 7$ The next perfect numbers are

$496 = 2^4 \times 31$ and $8128 = 2^4 \times 508 = 2^6 \times 127$

Theorem (~~Euler~~) If $2^{n+1}-1$ is prime then $2^n(2^{n+1}-1)$ is a perfect number

Proof $\int 2^n = 1 + \dots + 2^n = 2^{n+1}-1$. Since $2^{n+1}-1$ is prime, $\int 2^{n+1}-1 = 2^{n+1}-1+1 = 2^{n+1}$

So $\int 2^n(2^{n+1}-1) = \int 2^n \times \int 2^{n+1}-1 = 2^{n+1}(2^{n+1}-1)$.

<u>Theorem</u> (Euler) Every even perfect number is of the form $2^n(2^{n+1}-1)$ where $2^{n+1}-1$ is prime.

<u>Proof</u> Suppose N is even and perfect. Then $N = 2^n A$ for some $n \in \mathbb{Z}_+$ and A odd.

$$\int N = \int 2^n A = \int 2^n \times \int A \quad \text{since } \gcd(2^n, A) = 1$$

$$\int N = (2^{n+1}-1)\int A = 2^{n+1}A = 2N$$

$\gcd(2^n, 2^{n+1}-1) = 1 \Rightarrow 2^{n+1} \mid \int A$ and $2^{n+1}-1 \mid A$

So $A = k(2^{n+1}-1)$ and $\int A = k2^{n+1}$

If $k > 1$ then $1, k, k(2^{n+1}-1)$ are all divisors of A

So $\int A \geq 1 + k + k(2^{n+1}-1) = 1 + k2^{n+1}$ X.

So $k = 1$ and $A = (2^{n+1}-1)$ and $\int A = 2^{n+1}$

If A is not prime then $\int A > 2^{n+1}$ so A is prime

So $N = 2^n(2^{n+1}-1)$ where $2^{n+1}-1$ is prime. $\square$

<u>Odd Perfect numbers</u>

It is unknown whether there are any odd perfect numbers. We shall look at some of the simple properties that are known.

Suppose that N is odd, $N \in \mathbb{Z}_+$, $N \geq 3$ and N is perfect. Then $N = \prod_{i=1}^{k} p_i^{n_i}$ for $k \in \mathbb{Z}_+$, odd distinct primes p_i and $n_i \in \mathbb{Z}_+$, $1 \leq i \leq k$

Since the $p_i^{n_i}$ are coprime for $1 \leq i \leq k$,

$$\sigma N = \prod_{i=1}^{k} \sigma p_i^{n_i}$$

$$\sigma p_i^{n_i} = 1 + \dots + p^{n_i} = \frac{p^{n_i+1} - 1}{p_i - 1}$$

$$\sigma N = 2N \implies \prod_{i=1}^{k} \frac{p_i^{n_i+1} - 1}{p_i - 1} = 2 \prod_{i=1}^{k} p_i^{n_i} \quad (1)$$

Here, both LHS and RHS are integers. Some information can be obtained from writing the equation like this. Other ways are

$$\prod_{i=1}^{k} \left(1 - \frac{1}{p_i^{n_i n}}\right) = 2 \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right) \quad (2)$$

and

$$\prod_{i=1}^{k} \left(\sum_{j=0}^{n_i} \frac{1}{p_i^j}\right) = 2 \quad (3)$$

From this we can obtain some information. Note that the LHS of (2) is < 1, so if equality holds then the RHS must also be ≤ 1

<u>Theorem</u> (Euler) If $N \in \mathbb{Z}_+ \setminus \{1, 2\}$ is odd perfect written $\prod_{i=1}^{k} p_i^{n_i}$ as shown, then $k \geq 3$, that is, N has at least three distinct prime factors

<u>Proof</u> From (2) we have, if $k = 1$ $\quad 1 - \frac{1}{p_1^{n_1+1}} = 2\left(1 - \frac{1}{p_1}\right)$

but $p_1 \geq 3 \implies 2\left(1 - \frac{1}{p_1}\right) \geq \frac{4}{3}$ and $1 - \frac{1}{p_1^{n_1+1}} < 1$

If $k=2$ we have

$$\left(1-\frac{1}{p_1^{n_1+1}}\right)\left(1-\frac{1}{p_2^{n_2+1}}\right) < 1 \text{ and}$$

$$2\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right) \geq 2\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right) = \frac{16}{15}$$

□

We can extract some extra information from this.

If $k=3$, it can be shown that there are only 3 possibilities for (p_1, p_2, p_3). These can be excluded. One might think that one could continue like this. However, all that is known in this line is that if N exists, it must have at least 9 distinct prime factors (Nielsen, 2006?) and must have at least 101 not-necessarily-distinct prime factors (Ochem-Rao, 2012?)

Considering ~~question~~ equation (1) also gives important information.

<u>Theorem</u> (Euler) Let p be an odd prime and $n \in \mathbb{Z}_+$. Then the integer $\frac{p^{n+1}-1}{p-1} \equiv 0 \mod 2$ (that is, is even)

$\iff n \equiv 1 \mod 2$ (that is, n is odd)

$$\frac{p^{n+1}-1}{p-1} \equiv 0 \mod 4 \iff p \equiv -1 \mod 4 \text{ and } n \equiv 1 \mod 2$$
$$\text{or } n \equiv -1 \mod 4$$

Consequently if N is perfect and written as before, then there is exactly one ~~n_i~~ i such that $n_i \equiv 1 \mod 2$. For this i, $p_i \equiv 1 \mod 4$ and $n_i \equiv 1 \mod 4$

Proof See Problem Sheet 3

Prime Numbers

Distribution problems concerning primes are an important branch of number theory. One of the most important and oldest results is:

Theorem There are infinitely many prime numbers.

Proof By contradiction. Suppose there are only finitely many positive primes p_i, $1 \le i \le n$.

Consider $N = \prod_{i=1}^{n} p_i + 1$. Then $p_i \nmid N$, $1 \le i \le n$.

By the FTA there is at least one prime p, $p \mid N$.

$p \ne p_i$ for $1 \le i \le n$ $\times$ □

This proof also shows that if p_n is the n'th prime, with $p_i < p_{i+1}$ $\forall i$, then $p_n \le \prod_{i=1}^{n-1} p_i + 1$,

This is an estimate, although not a very good one.

One of the oldest methods for finding primes is the Sieve of Eratosthenes. The first prime is $p_1 = 2$. The second is $p_2 = 3$.

To find p_{n+1}, cross out all proper multiples of p_i, $1 \le i \le n$.

p_{n+1} is the smallest number after p_n which is not crossed out.

Another method which works well for small numbers is:

Theorem If $N \in \mathbb{Z}_+ \setminus \{1\}$ is not prime, then there is a +ve prime $p \le \sqrt{N}$ with $p \mid N$.

<u>Proof</u> If N is not prime then $N = kl$ for some $1 < k \leq l < N$. We can assume w.l.g. that k is prime and $k^2 \leq kl \leq N$. □

<u>Example</u> 709 is prime. To see this:

$23^2 = 529 < 709 \quad 29^2 = 841 > 709$.

Clearly 709 is not divisible by 2, 3, 5

$709 \equiv 2 \bmod 7$, $5 \bmod 11$, $7 \bmod 13$, $12 \bmod 17$, $3 \bmod 19$, $19 \bmod 23$.

So 709 is prime.

<u>Twin primes</u> All primes apart from 2 are <u>odd</u>. Apart from 3, 5, 7 there are never more than 2 consecutive odd primes (problem sheet 1). <u>Twin primes</u> are consecutive odd primes ≥ 11 e.g. 11, 13 ; 17, 19; 29, 31; 41, 43 ...

<u>Twin prime conjecture</u> There are infinitely many twin primes.

<u>Def^n</u> Let $p_1 < p_2 \ldots$ be the (positive) primes in increasing order. A <u>prime gap</u> is a set of <u>composite</u> (non-prime) integers between 2 primes, that is, of the form $\{k \in \mathbb{Z}_+ : p_n < k < p_{n+1}\}$ for some $n \geq 2$ e.g. $\{4\} = \{k \in \mathbb{Z}_+ : 3 < k < 5\}$

$\{6\} = \{k \in \mathbb{Z}_+ : 5 < k < 7\}$ $\quad \{8, 9, 10\} = \{k \in \mathbb{Z}_+ : 7 < k < 11\} \ldots$

Theorem (Problem Sheet 1) There are arbitrarily large prime gaps.

The length of the prime gap $\{k \in \mathbb{Z}_+ : p_n < k < p_{n+1}\}$ is $p_{n+1} - p_n$. This is always even, and since the number of integers in the gap is one less, there is always an odd number of integers in any prime gap.

Conjecture There is a prime gap of every even length ≥ 2.

How many primes are there? Since there are infinitely many the question really is: what can we say about the number of primes $\leq n$, or about the size of p_n...

The function $\pi(x)$

for any $x \in \mathbb{R}$, $\pi(x)$ is the number of positive primes $\leq x$

$$\begin{aligned}\pi(x) &= 0 \quad \text{for } x < 2 \\ &= 1 \quad 2 \leq x < 3 \\ &= 2 \quad 3 < x \leq 5 \ldots\end{aligned}$$

Prime number Theorem

$$\lim_{x \to +\infty} \frac{\pi(x)}{x/\log x} = 1$$

This was first proved in the 19th century using complex analysis.

This is an important result in analytic number theory and will not be proved in this course. But ~~so~~ some very ~~close~~ estimates of Chebyshev, which go some distance to proving this, and are used as the basis of a famous 20th Century proof of the PNT due to ~~Douglas~~ Donald Newman, will be looked at.

D. Newman. Amer. Math Monthly 1980

<u>Lemma</u> $\lim_{x \to +\infty} \frac{\pi(x)}{x/\ln x} = \lim_{n \to \infty} \frac{\pi(p_n)}{p_n/\ln p_n}$ if either limit exists ~~and is non zero~~

<u>Proof</u> If the first limit exists, of course the second one does as well. If $f(x) = \frac{x}{\ln x}$ then $f'(x) = \frac{1}{\ln(x)}\left(1 - \frac{1}{\ln x}\right) > 0$

if $x > e$. So $\frac{\pi(p_{n+1}) - 1}{p_{n+1}/\ln p_{n+1}} < \frac{\pi(x)}{x/\ln x} < \frac{\pi(p_n)}{p_n/\ln p_n} \quad \forall p_n < x < p_{n+1}$

Since $\lim_{x \to +\infty} \frac{x}{\ln x} = +\infty$ and hence $\lim_{n \to \infty} \frac{p_n}{\ln p_n} = +\infty$, the result follows.

<u>Lemma</u> $\lim_{n \to \infty} \frac{\pi(p_n)}{p_n/\ln p_n} = \lim_{n \to \infty} \frac{n \ln n}{p_n}$ if either limit exists and is non zero.

<u>Proof</u> $\frac{\pi(p_n)}{p_n/\ln p_n} = \frac{n \ln p_n}{p_n}$ If $\lim_{n \to \infty} \frac{n \ln p_n}{p_n} = c$ or $\lim_{n \to \infty} \frac{n \ln n}{p_n} = c$

for $c > 0$ then $\lim_{n \to \infty} (\ln n + \ln \ln p_n - \ln p_n) = \ln c$ or $\lim_{n \to \infty} (\ln n + \ln \ln n - \ln p_n) = \ln c$

These give $\lim_{n\to\infty}\left(\frac{\ln n}{\ln p_n}-1\right)=0$ or $\lim_{n\to\infty}\left(\frac{\ln p_n}{\ln n}-1\right)=0$

Either way, $\lim_{n\to\infty}\frac{\ln n}{\ln p_n}=\lim_{n\to\infty}\frac{\ln p_n}{\ln n}=1$

So $\lim_{n\to\infty}\frac{n\ln p_n}{p_n}=\lim_{n\to\infty}\frac{n\ln n}{p_n}$ if either exists.

<u>Corollary</u> $\lim_{x\to+\infty}\frac{\pi(x)}{x/\ln x}=1 \iff \lim_{n\to\infty}\frac{n\ln n}{p_n}=1.$

Before looking at Chebyshev's estimates in detail, we will look at some related examples. What Chebyshev used was a way of calculating the ~~number of divisors~~ power or any, of given prime dividing a factorial, or binomial coefficient.

<u>Example</u> Find the number of zeros at the end of the number 217! (written in the usual base 10 expansion)

To do this we need to find the maximal m_1 and m_2 such that $2^{m_1} \mid 217!$ and $5^{m_2} \mid 217$

then $10^{\min(m_1,m_2)} \mid 217!$ and the number of zeros at the end of 217! is $\min(m_1,m_2)$.

There are $\frac{216}{2}=108$ numbers ≤ 217 divisible by 2.

But some of these are divisible by 2^2, in fact 54 of them.

Of these, 27 are divisible by 2^3

$13 = \left\lfloor \frac{217}{16} \right\rfloor$ are divisible by 2^4

$6 = \left\lfloor \frac{217}{32} \right\rfloor$ divisible by 2^5

$3 = \left\lfloor \frac{217}{64} \right\rfloor$ divisible by 2^6

$1 = \left\lfloor \frac{217}{128} \right\rfloor$ divisible by 2^7

Here $\left\lfloor \frac{n}{m} \right\rfloor$ is the largest integer $\leq \frac{n}{m}$ if $n, m \in \mathbb{N}$, $m > 0$

So $m_1 = 108 + 54 + 27 + 13 + 6 + 3 + 1 = 212$

Similarly $m_2 = \left\lfloor \frac{217}{5} \right\rfloor + \left\lfloor \frac{217}{25} \right\rfloor + \left\lfloor \frac{217}{125} \right\rfloor$

$= 43 + 8 + 1 = 51$

So the number of zeros at the end of $217!$ is 51.

<u>Example</u> Find the number of zeros at the end of $\binom{217}{33}$

$= \frac{217 \times \cdots 185}{1 \times \cdots \times 33}$

Once again the number of zeros is Min (m_1, m_2), where 2^{m_1} and 5^{m_2} are the maximum powers of 2, 5 which divide $\binom{217}{33}$. There are 16 even numbers between 1 + 33 and 16 even between 185 and 217

There are 8 numbers divisible by 4 between 1 and 33 and

$\left(\frac{216 - 188 + 4}{4}\right) = 1 + \frac{28}{4} = 8$ between 185 + 217

(25)

4 divisible by 8 between 1 and 33

$\frac{216-192}{8} + 1 = 4$ between 185 and 217

2 divisible by 16 between 1 and 33 and 2 (192, 208)

between 185 and 217

32 and 192 divisible by 2^5.

But 192 is also divisible by 2^6

~~So $\binom{217}{33}$ is actually an odd number. So we need~~

So $m_1 = 1$

~~to look no further.~~ ~~We must have $Min(m_1, m_2) = 0$~~

Now we will look at m_2, to see what happens.

$\left\lfloor \frac{33}{5} \right\rfloor = 6$ But there are $\frac{215-185}{5} + 1 = 7$

numbers from 185 to 217 which are divisible by 5

$\left\lfloor \frac{33}{25} \right\rfloor = 1$ 200 is the only number between

185 and 217 which is divisible by $25 = 5^2$

So $m_2 = (7+1) - (6+1) = 1$.

So $Min(m_1, m_2) = 1$

By a similar method we can show $\binom{249}{33}$ is

odd ~~and the last digit is 5~~

Chebyshev's upper and lower bounds.

For constants $C_1 > C_2 > 0$, Chebyshev proved

$$C_2 \frac{x}{\ln x} \leq \pi(x) \leq C_1 \frac{x}{\ln x}$$ for all sufficiently large x.

C_1 and C_2 can be taken closer together by taking x larger - but the method he used does not allow C_1 and C_2 to be taken arbitrarily close to 1, however large x is.

The main step in the upper bound is:

<u>Theorem</u> $\pi(2n) - \pi(n) \leq \frac{2n\ln 2}{\ln n}$ $\forall n \in \mathbb{Z}_+$.

<u>Proof</u> $2^{2n} = \sum_{k=0}^{2n} \binom{2n}{k} 1^k$

So $\binom{2n}{n} < 2^{2n}$

$$2^{2n} > \binom{2n}{n} = \frac{2n(2n-1)\cdots(n+1)}{1\times\cdots\times n} > \prod_{\substack{p \text{ prime} \\ n<p\leq 2n}} p > n^{\pi(2n)-\pi(n)}$$

This is because if p is prime, $n < p \leq 2n$, then $p \mid 2n(2n-1)\cdots(n+1)$ but $p \nmid n!$ So $p \mid \binom{2n}{n}$

So $(\pi(2n) - \pi(n))\ln n < 2n\ln 2$ ☐

We also have $\pi(2n+1) - \pi(n+1) < \frac{(2n+1)\ln 2}{\ln(n+1)}$ by the same method: $2^{2n+1} > \binom{2n+1}{n+1}$

(27)

Since $\frac{x}{\ln x}$ is an increasing function for $x \geq e$

it follows that

$$\pi(x) - \pi(\tfrac{x}{2}) - 1 \leq \frac{x \ln 2}{\ln(x/2)} \qquad \forall x \in [e, \infty)$$

(This means x is real)

So $$\frac{\pi(x)\ln x}{x} < \frac{\ln x}{\ln(x/2)}\left(\frac{1}{2}\frac{\pi(x/2)\ln(x/2)}{x/2} + \ln 2\right) + \frac{\ln x}{x}$$

Writing $g(x) = \pi(x)\frac{\ln x}{x}$,

$$g(x) < \frac{\ln x}{\ln x - \ln 2}\left(\frac{1}{2}g(\tfrac{x}{2}) + \ln 2\right) + \frac{\ln x}{x}$$

So if $g(\frac{x}{2}) < C$ we have $g(x) < C$ provided that

$$\frac{\ln x}{\ln x - \ln 2}\left(\frac{C}{2} + \ln 2\right) + \frac{\ln x}{x} < C$$

It is not possible to do this for $C \leq 2\ln 2$.

It is possible to show e.g. $g(x) < 2 \quad \forall x \geq 2$.

This was on last year's problem sheet 3.

Chebyshev's lower bound

Theorem $\pi(n) > \frac{n \ln 2}{\ln n} - 1 \ \forall n \in \mathbb{Z}_+, n \geq 2.$

Proof Again we use $2^n = \sum_{k=0}^{n} \binom{n}{k}$.

Then the aim is to find an upper bound on $\binom{n}{k}$

by bounding the power of each prime p which can

divide $\binom{n}{k}$ – in exactly the same way as we did in

explicit exaples.

If p is prime and $p \mid \binom{n}{k}$, then $p \leq n$.

Then p divides $\lfloor \frac{k}{p} \rfloor$ of the integers between 1 and k

p divides at most $\lfloor \frac{k}{p} \rfloor + 1$ of the integers

$n-k+1$ to n inclusive.

p^l can only divide $k!$ if $p^l \leq k \leq n$ and then p^l divides

$\lfloor \frac{k}{p^l} \rfloor$ of the integers between 1 and k and whenever $p^l \leq n$,

p^l can divide at most $\lfloor \frac{k}{p^l} \rfloor + 1$ of the integers $n-k+1$ to n

inclusive and only if $p^l \leq n$ ~~$\iff$~~ ~~$l \leq \frac{\ln n}{\ln p}$~~

So the maximum power of p dividing n is $\underbrace{p \times \cdots \times p}_{l \text{ times}}$ where $p^l \leq n$

So the maximum power of p dividing $\binom{n}{k}$ is ~~$e^{\frac{\ln n}{\ln p}}$~~ p^l for l with $p^l \leq n$

So $\binom{n}{k} \leq \prod_{\substack{p \text{ prime} \\ p \leq n}} n = n^{\pi(n)}$

So $2^n = 2 + \sum_{k=1}^{n-1} \binom{n}{k} \leq 2 + (n-1).\, n^{\pi(n)} < n^{\pi(n)+1}$ $\forall n \geq 2$

So $n \ln 2 < (\pi(n)+1)\ln n$

and $\pi(n) > \frac{n \ln 2}{\ln n} - 1$ $\forall n \geq 2$

Riemann Zeta Function

$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$ is defined for all real $s > 1$

It is also defined for all $s \in \mathbb{C}$ with $Re(s) > 1$ if we define

$n^{-s} = e^{-s \ln n}$.

The Riemann zeta function is very important in more advanced theory of distribution of primes.

There is an alternative expression of $\zeta(s)$ as an infinite product. This expression is due to Euler.

<u>Theorem</u>

$\zeta(s) = \prod_{p \text{ prime}} (1-p^{-s})^{-1}$ $\forall s > 1$ (and $\forall s \in \mathbb{C}$ with $Re(s) > 1$)

<u>Proof</u> $(1-p^{-s})^{-1} = \sum_{k=0}^{\infty} p^{-sk}$

But if $n \in \mathbb{Z}_+$ then $n = \prod_{i=1}^{r} p_i^{k_i}$ for some $r \in \mathbb{Z}_+$, p_i prime, $k_i \in \mathbb{Z}_+$ $1 \leq i \leq r$

So $n^{-s} = \prod_{i=1}^{r} p_i^{-k_i s}$

So $\prod_{p \text{ prime}} \left(\sum_{k=0}^{\infty} p^{-sk} \right) = \sum_{n=1}^{\infty} n^{-s}$ $\quad Re(s) > 1$

i.e. $\zeta(s) = \sum_{n=1}^{\infty} n^{-s} = \prod_{p \text{ prime}} (1-p^{-s})^{-1}$ $\square$.

Also $\prod_{\substack{p \text{ prime} \\ p \leq n}} (1-p^{-1})^{-1} \longrightarrow \infty$ as $n \to \infty$.

In fact $\prod_{\substack{p \text{ prime} \\ p \leq n}} (1-p^{-1})^{-1} = \prod_{\substack{p \text{ prime} \\ p \leq n}} \left(\sum_{k=0}^{\infty} p^{-k} \right) \geq \sum_{m=1}^{n} \frac{1}{m} \to \infty$ as $m \to \infty$

So $\ln \left(\prod_{\substack{p \text{ prime} \\ p \leq n}} (1-p^{-1})^{-1} \right) \longrightarrow \infty$ as $n \to \infty$

$$\sum_{\substack{p \leq n \\ p \text{ prime}}} -\ln(1-p^{-1}) \longrightarrow \infty \text{ as } n \to \infty$$

$$-\ln(1-p^{-1}) = \frac{1}{p} - \frac{1}{2p^2} \cdots > \frac{1}{2p} \quad \forall p \geq 2$$

So $\sum_{\substack{p \leq n \\ p \text{ prime}}} \frac{1}{p} \longrightarrow \infty$ as $n \to \infty$