Perfect Numbers

Euler used the notation ~~to~~ $\int n$ to denote the ~~sum~~ 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 $a_1 \mid a$ and $b_1 \mid b$ $a_1, b_1 > 0$ in exactly one way

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

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 $\int 2^n = 1 + \cdots + 2^n = 2^{n+1} - 1$. 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 $k \geqslant 1$ then $1, k, k(2^{n+1}-1)$ are all divisors of A

So $\int A \geqslant 1 + k + k(2^{n+1}-1) = 1 + k2^{n+1}$ 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, $N \in \mathbb{Z}_+$, $N \geqslant 3$ 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 $1 \le i \le k$,

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

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

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

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

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

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 $\cancel{\geq}\ \leq 1$

<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

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

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

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 $\dfrac{p^{n+1}-1}{p-1} \equiv 0 \mod 2$ (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 $n_i \equiv 1 \mod 4$

<u>Proof</u> 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 $1 \le i \le n$ $\times$ $\square$

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 values is:

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

Proof 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 $k^2 \leq kl \leq N$. $\square$

Example 709 is prime To see this:

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

Clearly 709 is not divisible by 2, 3, 5

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

So 709 is prime.

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

Twin prime conjecture There are infinitely many twin primes.

Def^n Let $p_1 < p_2 \ldots$ be the (positive) primes in increasing order. A prime gap is a set of composite (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. $\{4\} = \{k \in \mathbb{Z}_+ : 3 < k < 5\}$
$\{6\} = \{k \in \mathbb{Z}_+ : 5 < k < 7\}$ $\quad \{8, 9, 10\} = \{k \in \mathbb{Z}_+ : 7 < k < 11\} \ldots$

<u>Theorem</u> (Problem Sheet 1) There are arbitrarily large prime gaps.

The <u>length</u> 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.

<u>Conjecture</u> 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...

<u>The function $\pi(x)$</u>

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

$$\pi(x) = 0 \quad \text{for } x < 2$$
$$= 1 \quad 2 \leq x < 3$$
$$= 2 \quad 3 < x \leq 5 \cdots$$

<u>Prime number Theorem</u>

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

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 ~~we~~ some very ~~clas~~ 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 $\frac{\pi(p_{n+1}) - 1}{p_{n+1}/\ln p_{n+1}} < \frac{\pi(x)}{x/\ln x} < \frac{\pi(p_n)}{p_n/\ln p_n}$ $\forall p_n < x < p_{n+1}$

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

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

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 $\text{Min}(m_1, m_2)$, 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

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 to look no further.~~ So $m_1 = 1$

~~We must have $Min(m_1, m_2) = 0$~~

~~However~~ Now, ~~the~~ we will look at ~~the max~~ 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 <u>similar method</u> we can show $\binom{249}{33}$ is

<u>odd</u> ~~and the last digit is 5~~

Chebyshev's upper and lower bounds.

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

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

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> $\pi(2n) - \pi(n) \leq \dfrac{2n\ln 2}{\ln n} \quad \forall n \in \mathbb{Z}_+.$

<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 $(\pi(2n) - \pi(n))\ln n < 2n \ln 2$ $\square$

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

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 examples.

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 $p^l \leq n$ ~~$\Leftrightarrow$~~ ~~$l \leq \frac{\ln n}{\ln p}$~~

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 ~~$\frac{\ln n}{\ln p}$~~ p^l for l with $p^l \leq n$

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

it follows that

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

(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.

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

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 theorems of distribution of primes.

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

Theorem

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

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

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

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 $n \longrightarrow \infty$.

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 $n \longrightarrow \infty$

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

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

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

The multiplicative group mod n

Let $n \in \mathbb{Z}_+$, $n \geq 1$

Def^n $\mathbb{Z}_n = \{k \bmod n : k \in \mathbb{Z}\}$

($\mathbb{Z}_n$ is an example of a quotient ring

$\mathbb{Z}_n = \mathbb{Z}/_{n\mathbb{Z}} = \{n\mathbb{Z} + k : k \in \mathbb{Z}\}$ where $n\mathbb{Z} = \{mn : m \in \mathbb{Z}\}$ is an ideal in $\mathbb{Z}$)

If $k_1 \equiv k_2 \bmod n$ and $m_1 \equiv m_2 \bmod n$ then

$k_1 + m_1 \equiv k_2 + m_2 \bmod n$ and $k_1 m_1 \equiv k_2 m_2 \bmod n$

So addition and multiplication in $\mathbb{Z}_n$ are well-defined

key $k_1 \bmod n + m_1 \bmod n = (k_1 + m_1) \bmod n$

$(k_1 \bmod n) . (m_1 \bmod n) = k_1 m_1 \bmod n$

Usually restrict to $n \geq 2$ so that $1 \bmod n \neq 0 \bmod n$

$1 \bmod n$ is an identity element $(k \bmod n)(1 \bmod n) = k \bmod n$

$\forall\, k \bmod n \in \mathbb{Z}_n$

$\mathbb{Z}_n$ is a commutative ring with identity (addition + multiplication are commutative)

Def^n $G_n = \{k \bmod n : \gcd(k, n) = 1\}$ is closed under multiplication

If $\gcd(k_1, n) = 1$ and $\gcd(k_2, n) = 1$ then $\gcd(k_1 k_2, n) = 1$

$\gcd(k, n) = 1 \iff \exists\, a, b \in \mathbb{Z}$ such that

$ak + bn = 1$ then $\gcd(a, n) = 1$ and

$(k \bmod n) . (a \bmod n) \equiv 1 - bn \equiv 1 \bmod n$

G_n is a multiplicative group. Each $k \bmod n \in G_n$ has

a multiplicative inverse $a \bmod n$ such that $ak \equiv 1 \bmod n$

For this reason, G_n is often known as the group of units mod n

Def^n The Euler phi-function $\phi(n)$ is defined for

$n \in \mathbb{Z}_+$ $\quad \phi(n) = \# \{k \in \mathbb{Z}_+ : 1 \le k \le n, \gcd(k,n) = 1\} = \#(G_n)$

$\phi(1) = 1$ by definition

$\phi(2) = 1 \quad \phi(3) = 2 \quad$ If p is prime, $\phi(p) = p-1$.

$\phi(n)$ is the number of elements of G_n

Examples $G_2 = \{1 \pmod 2\}$ $\quad G_3 = \{1, 2\}$ $\quad$ (we drop "mod n" if the context is clear)

$G_4 = \{1, 3\}$ because $2 \notin G_4$, $\gcd(2,4) = 2$

Def^n $k \bmod n \in \mathbb{Z}_n$ (or $k \in \mathbb{Z}_n$) is a zero-divisor if

$k \not\equiv 0 \bmod n$ and $kl \equiv 0 \bmod n$ for some $l \not\equiv 0 \bmod n$.

Example $2 \in \mathbb{Z}_4$ is a zero divisor because $2 \not\equiv 0 \bmod 4$

but $2 \times 2 \equiv 0 \bmod 4$

$k \in \mathbb{Z}_n$, $0<k<n$ is a zero divisor, $\Leftrightarrow$ $\gcd(k,n) > 1$ because

If $\gcd(k,n) = d$ then $k = k_1 d$, $n = n_1 d$ and $n_1 \not\equiv 0 \bmod n$

and $kn_1 \equiv 0 \bmod n$

Conversely $0 < k < n$ and $kl \equiv 0 \bmod n$ for $0 < l < n$

then $n = k_1 l_1$ where $k_1 | k$, $l_1 | l$ $\quad 1 \le k_1 \le k < n$,

$1 \le l_1 \le l < n$. Then $n = k_1 l_1 \Rightarrow 1 < k_1, l_1$, so

$\gcd(k,n) \ge k_1 > 1$ (and $\gcd(l,n) \ge l_1 > 1$)

Notation $\mathbb{Z}_n^* = \{k \bmod n : k \not\equiv 0 \bmod n\}$

If n is prime then $\mathbb{Z}_n^* = G_n$

Group axioms

A set G is a group if there is a binary operation $(g,h) \longmapsto gh : G\times G \to G$ satisfying the following axioms

Associativity $(gh)k = g(hk) \quad \forall\, g,h,k \in G$

Identity element $\exists\, 1 \in G$ s.t. $g1 = 1g = g \;\forall g \in G$

Inverses $\forall\, g \in G \;\exists\, g^{-1} \in G$ s.t. $gg^{-1} = g^{-1}g = 1$

The group is commutative or abelian if in addition the following property holds

Commutativity

$$gh = hg \quad \forall\; g, h \in G.$$

The binary operation is usually called multiplication but sometimes in a commutative group it is called addition. If it is called multiplication it can be written

$$gh \text{ or } g.h \text{ or } g\times h.$$

If it is called addition it is written $g+h$, the identity element is written as 0 and the inverse of g is written as $-g$.

Examples G_n is a finite commutative group under multiplication mod n.

Product Group

If G and H are groups we can define the product group (of G and H)

$$G \times H = \{(g,h) : g \in G, h \in H\}$$ with

multiplication (the binary operation) defined by

$$(g_1, h_1) \cdot (g_2, h_2) = (g_1 g_2, h_1 h_2)$$

The group axioms are satisfied

1. This multiplication is associative
2. $(1,1)$ is the identity element of $G \times H$
3. (g^{-1}, h^{-1}) is the inverse ~~element~~ of (g, h)

Similarly we can define the product $H_1 \times \dots \times H_r$ of groups H_i, $1 \leq i \leq r$

Examples $G_3 \times G_5$ and $G_2 \times G_3 \times G_5$ are groups.

Product groups are useful in classifying groups and in particular in determining when two groups are the same.

Homomorphisms and Isomorphisms

Let G and H be groups

Def^n $\psi : G \longrightarrow H$ is a (group) homomorphism

if $\psi(g_1 g_2) = \psi(g_1)\psi(g_2)$ $\forall g_1, g_2 \in G$.

It follows from this that $\psi(1_G) = 1_H$

where 1_G and 1_H are the identity elements of G and H and $\psi(g^{-1}) = (\psi(g))^{-1}$ $\forall g \in G$.

Def^n ψ is an isomorphism if ψ is a homomorphism and also a bijection. If ψ is an isomorphism then $\psi^{-1} : H \longrightarrow G$ is defined and is also a homomorphism - and an isomorphism.

Examples Let $m | n$ Then $\psi : \mathbb{Z}_n \longrightarrow \mathbb{Z}_m$ is preserves multiplication if ψ is defined by

$$\psi(k \bmod n) = k \bmod m$$

$$\gcd(k,n) = 1 \implies \gcd(k,m) = 1.$$

So $\psi(G_n) \subset G_m$ and $\psi : G_n \longrightarrow G_m$

is a group homomorphism

To see that ψ is well-defined.

if $x_1 \equiv x_2 \bmod n$ then

$n \mid x_1 - x_2$ and hence $m \mid x_1 - x_2$

and $x_1 \equiv x_2 \bmod m$.

Non Example Define $\psi : G_n \to \mathbb{C}$ by $\psi(k \bmod n) = e^{2\pi i k/n}$. ψ is an injective map (not homomorphism) whose image is the ~~group~~ set of primitive n'th roots of unity $\{z : z^n = 1,\ z^m \neq 1,\ 0 < m < n\}$

Examples If $n_i \mid n$ for $1 \leq i \leq r$ then

$\psi : \mathbb{Z}_n \longrightarrow \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_r}$ is well-defined

and preserves multiplication where

$\psi(x \bmod n) = (x \bmod n_1, \ \ldots \ x \bmod n_r)$

Once again $\gcd(x, n) = 1 \Rightarrow \gcd(x, n_i) = 1$ for $1 \leq i \leq r$.

So $\psi(G) \subset G_1 \times \cdots \times G_r$.

Theorem If $n = n_1 \times \cdots \times n_r$ and $\gcd(n_i, n_j) = 1$ for $i \neq j$ $1 \leq i, j \leq r$ then

$\psi : \mathbb{Z}_n \longrightarrow \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_r}$ defined as above

is a bijection and is an isomorphism from

G_n to $G_{n_1} \times \cdots \times G_{n_r}$

Proof $\mathbb{Z}_n$ and $\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_r}$ both have $n = n_1 \times \cdots \times n_r$ elements. So ψ is a bijection from $\mathbb{Z}_n$ to $\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_r}$

if it is injective

To show that ψ is <u>injective</u>:

Suppose $x \equiv y \bmod n_i$ for $1 \le i \le r$

Then $n_i \mid x-y$ $\quad 1 \le i \le r$

Since all n_i are coprime the lcm of the n_i is $n = n_1 \times \dots \times n_r$

So $n \mid x-y$ (by defn of lcm)

That is $x \equiv y \bmod n$

So ψ is <u>injective</u>

To show $\psi(G_n) = G_{n_1} \times \dots \times G_{n_r}$:

Every element of $\mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_r}$ is of the form $(x \bmod n_1, \dots x \bmod n_r)$ since ψ is a bijection onto $\mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_r}$. Such an element is in $G_{n_1} \times \dots \times G_{n_r} \iff \gcd(x, n_i) = 1 \quad 1 \le i \le r$.

But if $\gcd(x, n_i) = 1$ for $1 \le i \le r$ then $\gcd(x, n) = 1$ and $x \bmod n \in G_n$.

So $\psi(G_n) = G_{n_1} \times \dots \times G_{n_r}$

$\square$.

<u>Corollary</u> If $n_1, \dots n_r$ are coprime then

$$\phi(n_1 \times \dots \times n_r) = \phi(n_1) \times \dots \times \phi(n_r)$$

<u>Proof</u> If $n = n_1 \times \dots \times n_r$ then G_n and $G_{n_1} \times \dots \times G_{n_r}$ are isomorphic. In particular they have the same

numbers of elements. These numbers are $\phi(n)$ and $\phi(n_1) \cdots \times \phi(n_r)$

So $\phi(n) = \phi(n_1) \cdots \times \phi(n_r)$

Examples $15 = 5 \times 3$

$\phi(15) = \phi(5) \times \phi(3) = (5-1)(3-1) = 8$

$G_{15} = \{1, 2, 4, 7, 8, 11, 13, 14\}$

To construct $\psi : \mathbb{Z}_{15} \to \mathbb{Z}_5 \times \mathbb{Z}_3$:

$0 \mapsto (0,0)$ $\quad 1 \mapsto (1,1)$ $\quad 2 \mapsto (2,2)$

$3 \mapsto (3,0)$ $\quad 4 \mapsto (4,1)$ $\quad 5 \mapsto (0,2)$

$6 \mapsto (1,0)$ $\quad 7 \mapsto (2,1)$ $\quad 8 \mapsto (3,2)$

$9 \mapsto (4,0)$ $\quad 10 \mapsto (0,1)$ $\quad 11 \mapsto (1,2)$

$12 \mapsto (2,0)$ $\quad 13 \mapsto (3,1)$ $\quad 14 \mapsto (4,2)$

Note that the image of G_{15} is $G_5 \times G_3$ as expected $G_5 \times G_3 = \{(l, k) : l \not\equiv 0 \bmod 5,\ k \not\equiv 0 \bmod 3\}$

<u>Example</u> To map $\mathbb{Z}_6$ to $\mathbb{Z}_3 \times \mathbb{Z}_2$ mode

$x \bmod 6 \mapsto (x \bmod 3,\ x \bmod 2)$

$0 \mapsto (0,0)$ $1 \mapsto (1,1)$ $2 \mapsto (2,0)$

$3 \mapsto (0,1)$ $4 \mapsto (1,0)$ $5 \mapsto (2,1)$

$G_6 = \{1, 5\}$ $\quad G_3 \times G_2 = \{(1,1)\ (2,1)\}$

	(1,1)	(2,1)
(1,1)	(1,1)	(2,1)
(2,1)	(2,1)	(1,1)

	1	5
1	1	5
5	5	1

<u>General formula for $\phi(n)$</u>

Write $n = \prod_{i=1}^{r} p_i^{k_i}$ where p_i are distinct primes

and $k_i > 0$

Then $\phi(n) = \prod_{i=1}^{r} \phi(p_i^{k_i})$ because $p_i^{k_i}$ ~~are cop~~ and $p_j^{k_j}$

are coprime for $i \neq j$. But ~~that~~ what is $\phi(p^k)$?

We know $\phi(p) = p-1$ if p is prime.

<u>Lemma</u> If p is prime, $\phi(p^k) = p^{k-1}(p-1)$

<u>Proof</u> $\phi(p^k) = \#\{m : 1 \le m \le p^k \ \gcd(m, p^k) = 1\}$

$= \#\{m : 1 \le m \le p^k : \gcd(m, p) = 1\}$

$= p^k - \#\{sp : 1 \le s \le p^k\} = p^k - \#\{s : 1 \le s \le p^{k-1}\}$

$= p^k - p^{k-1} = p^{k-1}(p-1)$

Example $\phi(4) = 2^2 - 2 = 2$

Confirmation: $G_4 = \{1, 3\}$ – 2 elements

Example $\phi(12) = \phi(2^2) \times \phi(3) = 2(2-1) \times 3-1 = 4$

$G_{12} = \{1, 5, 7, 11\}$

Congruence Equations

A ~~congruence eq~~ linear congruence equation is one of the form

$$ax \equiv b \mod n \qquad (1)$$

A system of linear congruence equations is a system of ~~the~~ equations

$$\left.\begin{aligned} a_1 x &\equiv b_1 \mod n_1 \\ &\vdots \\ a_r x &\equiv b_r \mod n_r \end{aligned}\right\} \quad (2)$$

Such equations or systems of equations may or may not have a solution. If (1) has a sol^n, it is of the form $x \equiv c \mod n$. If (2) has a sol^n, it is of the form $x \equiv c \mod n$ where $n = \text{lcm}(n_1, \ldots n_r)$

Example Find the multiplicative inverse of $7 \in G_{12}$.
This can be written as: Solve

$$7x \equiv 1 \mod 12$$

The sol^n is $x \equiv 7 \mod 12$ since $7 \times 7 \equiv 1 \mod 12$. This solution is unique.